

Alexey L. Gorodentsev

Algebra I

Textbook for Students of Mathematics



Springer

Algebra I

Alexey L. Gorodentsev

Algebra I

Textbook for Students of Mathematics



Springer

Alexey L. Gorodentsev
Faculty of Mathematics
National Research University
“Higher School of Economics”
Moscow, Russia

Originally published in Russian as “Algebra. Uchebnik dlya studentov-matematikov. Chast’ I”, © MCCME 2013

ISBN 978-3-319-45284-5 ISBN 978-3-319-45285-2 (eBook)
DOI 10.1007/978-3-319-45285-2

Library of Congress Control Number: 2016959261

Mathematics Subject Classification (2010): 11.01, 12.01, 13.01, 14.01, 15.01, 16.01, 18.01, 20.01

© Springer International Publishing AG 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This is the first part of an intensive 2-year course of algebra for students beginning a professional study of higher mathematics. This textbook is based on courses given at the Independent University of Moscow and at the Faculty of Mathematics in the National Research University Higher School of Economics. In particular, it contains a large number of exercises that were discussed in class, some of which are provided with commentary and hints, as well as problems for independent solution, which were assigned as homework. Working out the exercises is of crucial importance in understanding the subject matter of this book.

Moscow, Russia

Alexey L. Gorodentsev

Contents

| | | |
|----------|---|-----------|
| 1 | Set-Theoretic and Combinatorial Background | 1 |
| 1.1 | Sets and Maps | 1 |
| 1.1.1 | Sets | 1 |
| 1.1.2 | Maps | 2 |
| 1.1.3 | Fibers of Maps | 3 |
| 1.2 | Equivalence Classes | 7 |
| 1.2.1 | Equivalence Relations | 7 |
| 1.2.2 | Implicitly Defined Equivalences | 9 |
| 1.3 | Compositions of Maps | 10 |
| 1.3.1 | Composition Versus Multiplication | 10 |
| 1.3.2 | Right Inverse Map and the Axiom of Choice | 11 |
| 1.3.3 | Invertible Maps | 12 |
| 1.3.4 | Transformation Groups | 12 |
| 1.4 | Posets | 13 |
| 1.4.1 | Partial Order Relations | 13 |
| 1.4.2 | Well-Ordered Sets | 15 |
| 1.4.3 | Zorn's Lemma | 15 |
| | Problems for Independent Solution to Chap. 1 | 16 |
| 2 | Integers and Residues | 19 |
| 2.1 | Fields, Rings, and Abelian Groups | 19 |
| 2.1.1 | Definition of a Field | 19 |
| 2.1.2 | Commutative Rings | 21 |
| 2.1.3 | Abelian Groups | 21 |
| 2.1.4 | Subtraction and Division | 23 |
| 2.2 | The Ring of Integers | 24 |
| 2.2.1 | Divisibility | 24 |
| 2.2.2 | The Equation $ax + by = k$ and the Greatest Common Divisor in \mathbb{Z} | 24 |
| 2.2.3 | The Euclidean Algorithm | 25 |
| 2.3 | Coprime Elements | 26 |

| | | |
|----------|---|-----------|
| 2.4 | Rings of Residues | 27 |
| 2.4.1 | Residue Classes Modulo n | 27 |
| 2.4.2 | Zero Divisors and Nilpotents | 28 |
| 2.4.3 | Invertible Elements in Residue Rings | 28 |
| 2.4.4 | Residue Fields | 29 |
| 2.5 | Direct Products of Commutative Groups and Rings | 30 |
| 2.6 | Homomorphisms | 31 |
| 2.6.1 | Homomorphisms of Abelian Groups | 31 |
| 2.6.2 | Kernel of a Homomorphism | 32 |
| 2.6.3 | Group of Homomorphisms | 32 |
| 2.6.4 | Homomorphisms of Commutative Rings | 33 |
| 2.6.5 | Homomorphisms of Fields | 34 |
| 2.7 | Chinese Remainder Theorem | 34 |
| 2.8 | Characteristic | 35 |
| 2.8.1 | Prime Subfield | 35 |
| 2.8.2 | Frobenius Endomorphism | 36 |
| | Problems for Independent Solution to Chap. 2 | 37 |
| 3 | Polynomials and Simple Field Extensions | 41 |
| 3.1 | Formal Power Series | 41 |
| 3.1.1 | Rings of Formal Power Series | 41 |
| 3.1.2 | Algebraic Operations on Power Series | 42 |
| 3.1.3 | Polynomials | 43 |
| 3.1.4 | Differential Calculus | 44 |
| 3.2 | Polynomial Rings | 46 |
| 3.2.1 | Division | 46 |
| 3.2.2 | Coprime Polynomials | 48 |
| 3.2.3 | Euclidean Algorithm | 48 |
| 3.3 | Roots of Polynomials | 50 |
| 3.3.1 | Common Roots | 50 |
| 3.3.2 | Multiple Roots | 51 |
| 3.3.3 | Separable Polynomials | 51 |
| 3.4 | Adjunction of Roots | 52 |
| 3.4.1 | Residue Class Rings | 52 |
| 3.4.2 | Algebraic Elements | 54 |
| 3.4.3 | Algebraic Closure | 55 |
| 3.5 | The Field of Complex Numbers | 55 |
| 3.5.1 | The Complex Plane | 55 |
| 3.5.2 | Complex Conjugation | 58 |
| 3.5.3 | Trigonometry | 58 |
| 3.5.4 | Roots of Unity and Cyclotomic Polynomials | 60 |
| 3.5.5 | The Gaussian Integers | 62 |
| 3.6 | Finite Fields | 62 |
| 3.6.1 | Finite Multiplicative Subgroups in Fields | 62 |
| 3.6.2 | Description of All Finite Fields | 63 |

| | | |
|----------|---|------------|
| 3.6.3 | Quadratic Residues | 65 |
| | Problems for Independent Solution to Chap. 3 | 66 |
| 4 | Elementary Functions and Power Series Expansions | 73 |
| 4.1 | Rings of Fractions | 73 |
| 4.1.1 | Localization | 73 |
| 4.1.2 | Field of Fractions of an Integral Domain | 75 |
| 4.2 | Field of Rational Functions | 76 |
| 4.2.1 | Simplified Fractions | 76 |
| 4.2.2 | Partial Fraction Expansion | 77 |
| 4.2.3 | Power Series Expansions of Rational Functions | 79 |
| 4.2.4 | Linear Recurrence Relations | 80 |
| 4.3 | Logarithm and Exponential | 82 |
| 4.3.1 | The Logarithm | 83 |
| 4.3.2 | The Exponential | 83 |
| 4.3.3 | Power Function and Binomial Formula | 84 |
| 4.4 | Todd's Series and Bernoulli Numbers | 88 |
| 4.4.1 | Action of $\mathbb{Q}[[d/dt]]$ on $\mathbb{Q}[t]$ | 88 |
| 4.4.2 | Bernoulli Numbers | 91 |
| 4.5 | Fractional Power Series | 92 |
| 4.5.1 | Puiseux Series | 92 |
| 4.5.2 | Newton's Method | 96 |
| | Problems for Independent Solution to Chap. 4 | 100 |
| 5 | Ideals, Quotient Rings, and Factorization | 103 |
| 5.1 | Ideals | 103 |
| 5.1.1 | Definition and Examples | 103 |
| 5.1.2 | Noetherian Rings | 104 |
| 5.2 | Quotient Rings | 106 |
| 5.2.1 | Factorization Homomorphism | 106 |
| 5.2.2 | Maximal Ideals and Evaluation Maps | 107 |
| 5.2.3 | Prime Ideals and Ring Homomorphisms to Fields | 108 |
| 5.2.4 | Finitely Generated Commutative Algebras | 109 |
| 5.3 | Principal Ideal Domains | 109 |
| 5.3.1 | Euclidean Domains | 109 |
| 5.3.2 | Greatest Common Divisor | 110 |
| 5.3.3 | Coprime Elements | 111 |
| 5.3.4 | Irreducible Elements | 111 |
| 5.4 | Unique Factorization Domains | 112 |
| 5.4.1 | Irreducible Factorization | 112 |
| 5.4.2 | Prime Elements | 114 |
| 5.4.3 | GCD in Unique Factorization Domains | 115 |
| 5.4.4 | Polynomials over Unique Factorization Domains | 116 |

| | | |
|----------|---|-----|
| 5.5 | Factorization of Polynomials with Rational Coefficients | 118 |
| 5.5.1 | Reduction of Coefficients | 118 |
| 5.5.2 | Kronecker's Algorithm | 119 |
| | Problems for Independent Solution to Chap. 5 | 120 |
| 6 | Vectors | 123 |
| 6.1 | Vector Spaces and Modules | 123 |
| 6.1.1 | Definitions and Examples | 123 |
| 6.1.2 | Linear Maps | 124 |
| 6.1.3 | Proportional Vectors | 125 |
| 6.2 | Bases and Dimension | 127 |
| 6.2.1 | Linear Combinations | 127 |
| 6.2.2 | Linear Dependence | 130 |
| 6.2.3 | Basis of a Vector Space | 132 |
| 6.2.4 | Infinite-Dimensional Vector Spaces | 134 |
| 6.3 | Space of Linear Maps | 135 |
| 6.3.1 | Kernel and Image | 135 |
| 6.3.2 | Matrix of a Linear Map | 136 |
| 6.4 | Vector Subspaces | 138 |
| 6.4.1 | Codimension | 138 |
| 6.4.2 | Linear Spans | 138 |
| 6.4.3 | Sum of Subspaces | 139 |
| 6.4.4 | Transversal Subspaces | 140 |
| 6.4.5 | Direct Sums and Direct Products | 141 |
| 6.5 | Affine Spaces | 142 |
| 6.5.1 | Definition and Examples | 142 |
| 6.5.2 | Affinization and Vectorization | 143 |
| 6.5.3 | Center of Mass | 143 |
| 6.5.4 | Affine Subspaces | 145 |
| 6.5.5 | Affine Maps | 148 |
| 6.5.6 | Affine Groups | 148 |
| 6.6 | Quotient Spaces | 149 |
| 6.6.1 | Quotient by a Subspace | 149 |
| 6.6.2 | Quotient Groups of Abelian Groups | 150 |
| | Problems for Independent Solution to Chap. 6 | 151 |
| 7 | Duality | 155 |
| 7.1 | Dual Spaces | 155 |
| 7.1.1 | Covectors | 155 |
| 7.1.2 | Canonical Inclusion $V \hookrightarrow V^{**}$ | 158 |
| 7.1.3 | Dual Bases | 158 |
| 7.1.4 | Pairings | 160 |
| 7.2 | Annihilators | 161 |

| | | |
|-----------|--|-----|
| 7.3 | Dual Linear Maps | 164 |
| 7.3.1 | Pullback of Linear Forms | 164 |
| 7.3.2 | Rank of a Matrix | 165 |
| | Problems for Independent Solution to Chap. 7 | 167 |
| 8 | Matrices | 173 |
| 8.1 | Associative Algebras over a Field | 173 |
| 8.1.1 | Definition of Associative Algebra | 173 |
| 8.1.2 | Invertible Elements | 174 |
| 8.1.3 | Algebraic and Transcendental Elements | 175 |
| 8.2 | Matrix Algebras | 175 |
| 8.2.1 | Multiplication of Matrices | 175 |
| 8.2.2 | Invertible Matrices | 179 |
| 8.3 | Transition Matrices | 180 |
| 8.4 | Gaussian Elimination | 182 |
| 8.4.1 | Elimination by Row Operations | 182 |
| 8.4.2 | Location of a Subspace with Respect to a Basis | 190 |
| 8.4.3 | Gaussian Method for Inverting Matrices | 192 |
| 8.5 | Matrices over Noncommutative Rings | 195 |
| | Problems for Independent Solution to Chap. 8 | 199 |
| 9 | Determinants | 205 |
| 9.1 | Volume Forms | 205 |
| 9.1.1 | Volume of an n -Dimensional Parallelepiped | 205 |
| 9.1.2 | Skew-Symmetric Multilinear Forms | 207 |
| 9.2 | Digression on Parities of Permutations | 208 |
| 9.3 | Determinants | 210 |
| 9.3.1 | Basic Properties of Determinants | 211 |
| 9.3.2 | Determinant of a Linear Endomorphism | 214 |
| 9.4 | Grassmannian Polynomials | 215 |
| 9.4.1 | Polynomials in Skew-Commuting Variables | 215 |
| 9.4.2 | Linear Change of Grassmannian Variables | 216 |
| 9.5 | Laplace Relations | 217 |
| 9.6 | Adjunct Matrix | 220 |
| 9.6.1 | Row and Column Cofactor Expansions | 220 |
| 9.6.2 | Matrix Inversion | 221 |
| 9.6.3 | Cayley–Hamilton Identity | 222 |
| 9.6.4 | Cramer’s Rules | 223 |
| | Problems for Independent Solution to Chap. 9 | 225 |
| 10 | Euclidean Spaces | 229 |
| 10.1 | Inner Product | 229 |
| 10.1.1 | Euclidean Structure | 229 |
| 10.1.2 | Length of a Vector | 230 |
| 10.1.3 | Orthogonality | 230 |

| | | |
|-----------|--|-----|
| 10.2 | Gramians | 233 |
| 10.2.1 | Gram Matrices | 233 |
| 10.2.2 | Euclidean Volume | 234 |
| 10.2.3 | Orientation | 234 |
| 10.2.4 | Cauchy–Bunyakovsky–Schwarz Inequality | 235 |
| 10.3 | Duality | 235 |
| 10.3.1 | Isomorphism $V \simeq V^*$ Provided by Euclidean Structure | 235 |
| 10.3.2 | Orthogonal Complement and Orthogonal Projection | 236 |
| 10.4 | Metric Geometry | 238 |
| 10.4.1 | Euclidean Metric | 238 |
| 10.4.2 | Angles | 242 |
| 10.5 | Orthogonal Group | 244 |
| 10.5.1 | Euclidean Isometries | 244 |
| 10.5.2 | Orthogonal Matrices | 244 |
| | Problems for Independent Solution to Chap. 10 | 248 |
| 11 | Projective Spaces | 253 |
| 11.1 | Projectivization | 253 |
| 11.1.1 | Points and Charts | 253 |
| 11.1.2 | Global Homogeneous Coordinates | 254 |
| 11.1.3 | Local Affine Coordinates | 255 |
| 11.2 | Polynomials Revisited | 258 |
| 11.2.1 | Polynomial Functions on a Vector Space | 258 |
| 11.2.2 | Symmetric Algebra of a Vector Space | 258 |
| 11.2.3 | Polynomial Functions on an Affine Space | 262 |
| 11.2.4 | Affine Algebraic Varieties | 262 |
| 11.3 | Projective Algebraic Varieties | 263 |
| 11.3.1 | Homogeneous Equations | 263 |
| 11.3.2 | Projective Closure of an Affine Hypersurface | 264 |
| 11.3.3 | Space of Hypersurfaces | 265 |
| 11.3.4 | Linear Systems of Hypersurfaces | 266 |
| 11.4 | Complementary Subspaces and Projections | 268 |
| 11.5 | Linear Projective Isomorphisms | 270 |
| 11.5.1 | Action of a Linear Isomorphism on Projective Space | 270 |
| 11.5.2 | Linear Projective Group | 271 |
| 11.6 | Cross Ratio | 272 |
| 11.6.1 | Action of the Permutation Group S_4 | 272 |
| 11.6.2 | Special Quadruples of Points | 273 |
| 11.6.3 | Harmonic Pairs of Points | 274 |
| | Problems for Independent Solution to Chap. 11 | 275 |
| 12 | Groups | 279 |
| 12.1 | Definition and First Examples | 279 |

| | | |
|-----------|--|------------|
| 12.2 | Cycles | 280 |
| 12.2.1 | Cyclic Subgroups | 280 |
| 12.2.2 | Cyclic Groups | 281 |
| 12.2.3 | Cyclic Type of Permutation | 281 |
| 12.3 | Groups of Figures | 283 |
| 12.4 | Homomorphisms of Groups | 289 |
| 12.5 | Group Actions | 294 |
| 12.5.1 | Definitions and Terminology | 294 |
| 12.5.2 | Orbits and Stabilizers | 295 |
| 12.5.3 | Enumeration of Orbits | 298 |
| 12.6 | Factorization of Groups | 300 |
| 12.6.1 | Cosets | 300 |
| 12.6.2 | Normal Subgroups | 300 |
| 12.6.3 | Quotient Groups | 301 |
| | Problems for Independent Solution to Chap. 12 | 303 |
| 13 | Descriptions of Groups | 309 |
| 13.1 | Generators and Relations | 309 |
| 13.1.1 | Free Groups | 309 |
| 13.1.2 | Presentation of a Group by Generators and Relators | 310 |
| 13.1.3 | Presentations for the Dihedral Groups | 312 |
| 13.1.4 | Presentations of the Groups of Platonic Solids | 313 |
| 13.2 | Presentation of the Symmetric Group | 318 |
| 13.2.1 | Complete Group of a Regular Simplex | 318 |
| 13.2.2 | Bruhat Order | 321 |
| 13.3 | Simple Groups and Composition Series | 324 |
| 13.3.1 | Jordan–Hölder Series | 324 |
| 13.3.2 | Finite Simple Groups | 326 |
| 13.4 | Semidirect Products | 328 |
| 13.4.1 | Semidirect Product of Subgroups | 328 |
| 13.4.2 | Semidirect Product of Groups | 329 |
| 13.5 | p -Groups and Sylow’s Theorems | 330 |
| 13.5.1 | p -Groups in Action | 330 |
| 13.5.2 | Sylow Subgroups | 331 |
| | Problems for Independent Solution to Chap. 13 | 332 |
| 14 | Modules over a Principal Ideal Domain | 335 |
| 14.1 | Modules over Commutative Rings Revisited | 335 |
| 14.1.1 | Free Modules | 336 |
| 14.1.2 | Generators and Relations | 337 |
| 14.1.3 | Linear Maps | 338 |
| 14.1.4 | Matrices of Linear Maps | 339 |
| 14.1.5 | Torsion | 341 |
| 14.1.6 | Quotient of a Module by an Ideal | 341 |
| 14.1.7 | Direct Sum Decompositions | 341 |
| 14.1.8 | Semisimplicity | 343 |

| | | |
|-----------|--|-----|
| 14.2 | Invariant Factors | 344 |
| 14.2.1 | Submodules of Finitely Generated Free Modules | 344 |
| 14.2.2 | Deduction of the Invariant Factors Theorem from the Smith Normal Form Theorem | 345 |
| 14.2.3 | Uniqueness of the Smith Normal Form | 346 |
| 14.2.4 | Gaussian Elimination over a Principal Ideal Domain | 346 |
| 14.3 | Elementary Divisors | 351 |
| 14.3.1 | Elementary Divisors Versus Invariant Factors | 351 |
| 14.3.2 | Existence of the Canonical Decomposition | 353 |
| 14.3.3 | Splitting Off Torsion | 353 |
| 14.3.4 | Splitting Off p -Torsion | 353 |
| 14.3.5 | Invariance of p -Torsion Exponents | 354 |
| 14.4 | Description of Finitely Generated Abelian Groups | 355 |
| 14.4.1 | Canonical Form of a Finitely Generated Abelian Group | 355 |
| 14.4.2 | Abelian Groups Presented by Generators and Relations | 356 |
| | Problems for Independent Solution to Chap. 14 | 356 |
| 15 | Linear Operators | 361 |
| 15.1 | Classification of Operators | 361 |
| 15.1.1 | Spaces with Operators | 361 |
| 15.1.2 | Invariant Subspaces and Decomposability | 361 |
| 15.1.3 | Space with Operator as a $\mathbb{k}[t]$ -Module | 362 |
| 15.1.4 | Elementary Divisors | 363 |
| 15.1.5 | Minimal Polynomial | 365 |
| 15.1.6 | Characteristic Polynomial | 366 |
| 15.2 | Operators of Special Types | 367 |
| 15.2.1 | Nilpotent Operators | 367 |
| 15.2.2 | Semisimple Operators | 368 |
| 15.2.3 | Cyclic Vectors and Cyclic Operators | 370 |
| 15.2.4 | Eigenvectors and Eigenvalues | 371 |
| 15.2.5 | Eigenspaces | 372 |
| 15.2.6 | Diagonalizable Operators | 372 |
| 15.2.7 | Annihilating Polynomials | 373 |
| 15.3 | Jordan Decomposition | 375 |
| 15.3.1 | Jordan Normal Form | 375 |
| 15.3.2 | Root Decomposition | 376 |
| 15.3.3 | Commuting Operators | 377 |
| 15.3.4 | Nilpotent and Diagonalizable Components | 378 |
| 15.4 | Functions of Operators | 379 |
| 15.4.1 | Evaluation of Functions on an Operator | 379 |
| 15.4.2 | Interpolating Polynomial | 381 |
| 15.4.3 | Comparison with Analytic Approaches | 383 |
| | Problems for Independent Solution to Chap. 15 | 384 |

| | | |
|-----------|---|-----|
| 16 | Bilinear Forms | 387 |
| 16.1 | Bilinear Forms and Correlations | 387 |
| 16.1.1 | Space with Bilinear Form | 387 |
| 16.1.2 | Gramians | 388 |
| 16.1.3 | Left Correlation | 389 |
| 16.1.4 | Nondegeneracy | 390 |
| 16.1.5 | Kernels | 390 |
| 16.1.6 | Nonsymmetric and (Skew)-Symmetric Forms | 391 |
| 16.1.7 | Characteristic Polynomial and Characteristic Values | 392 |
| 16.2 | Nondegenerate Forms | 395 |
| 16.2.1 | Dual Bases | 395 |
| 16.2.2 | Isotropic Subspaces | 395 |
| 16.2.3 | Isometry Group | 396 |
| 16.2.4 | Correspondence Between Forms and Operators | 396 |
| 16.2.5 | Canonical Operator | 397 |
| 16.3 | Adjoint Operators | 399 |
| 16.3.1 | Reflexive Operators | 400 |
| 16.4 | Orthogonals and Orthogonal Projections | 403 |
| 16.4.1 | Orthogonal Projections | 403 |
| 16.4.2 | Biorthogonal Direct Sums | 405 |
| 16.4.3 | Classification of Nondegenerate Forms | 405 |
| 16.5 | Symmetric and Skew-Symmetric Forms | 408 |
| 16.5.1 | Orthogonals and Kernel | 409 |
| 16.5.2 | Orthogonal Projections | 409 |
| 16.5.3 | Adjoint Operators | 411 |
| 16.5.4 | Form–Operator Correspondence | 411 |
| 16.6 | Symplectic Spaces | 411 |
| 16.6.1 | Symplectic Group | 412 |
| 16.6.2 | Lagrangian Subspaces | 413 |
| 16.6.3 | Pfaffian | 414 |
| | Problems for Independent Solution to Chap. 16 | 416 |
| 17 | Quadratic Forms and Quadrics | 421 |
| 17.1 | Quadratic Forms and Their Polarizations | 421 |
| 17.1.1 | Space with a Quadratic Form | 421 |
| 17.1.2 | Gramian and Gram Determinant | 422 |
| 17.1.3 | Kernel and Rank | 423 |
| 17.1.4 | Sums of Squares | 423 |
| 17.1.5 | Isotropic and Anisotropic Subspaces | 424 |
| 17.1.6 | Hyperbolic Forms | 425 |
| 17.2 | Orthogonal Geometry of Nonsingular Forms | 427 |
| 17.2.1 | Isometries | 427 |
| 17.2.2 | Reflections | 428 |

| | | |
|-----------|--|-----|
| 17.3 | Quadratic Forms over Real and Simple Finite Fields..... | 431 |
| 17.3.1 | Quadratic Forms over $\mathbb{F}_p = \mathbb{Z}/(p)$ | 432 |
| 17.3.2 | Real Quadratic Forms..... | 433 |
| 17.3.3 | How to Find the Signature of a Real Form..... | 434 |
| 17.4 | Projective Quadrics..... | 435 |
| 17.4.1 | Geometric Properties of Projective Quadrics..... | 435 |
| 17.4.2 | Smooth Quadrics..... | 440 |
| 17.4.3 | Polarities..... | 443 |
| 17.5 | Affine Quadrics..... | 444 |
| 17.5.1 | Projective Enhancement of Affine Quadrics..... | 444 |
| 17.5.2 | Smooth Central Quadrics..... | 447 |
| 17.5.3 | Paraboloids..... | 448 |
| 17.5.4 | Simple Cones..... | 449 |
| 17.5.5 | Cylinders..... | 450 |
| | Problems for Independent Solution to Chap. 17..... | 454 |
| 18 | Real Versus Complex | 459 |
| 18.1 | Realification..... | 459 |
| 18.1.1 | Realification of a Complex Vector Space..... | 459 |
| 18.1.2 | Comparison of Linear Groups..... | 459 |
| 18.2 | Complexification..... | 462 |
| 18.2.1 | Complexification of a Real Vector Space..... | 462 |
| 18.2.2 | Complex Conjugation..... | 463 |
| 18.2.3 | Complexification of Linear Maps..... | 463 |
| 18.2.4 | Complex Eigenvectors..... | 464 |
| 18.2.5 | Complexification of the Dual Space..... | 465 |
| 18.2.6 | Complexification of a Bilinear Form..... | 465 |
| 18.3 | Real Structures..... | 466 |
| 18.4 | Complex Structures..... | 467 |
| 18.5 | Hermitian Enhancement of Euclidean Structure..... | 469 |
| 18.5.1 | Hermitian Structure..... | 469 |
| 18.5.2 | Kähler Triples..... | 471 |
| 18.5.3 | Completing Kähler Triples for a Given Euclidean Structure..... | 472 |
| 18.6 | Hermitian Enhancement of Symplectic Structure..... | 473 |
| 18.6.1 | Completing Kähler Triples for a Given Symplectic Structure..... | 473 |
| 18.6.2 | Siegel Upper Half-Space and Riemann Relations..... | 476 |
| | Problems for Independent Solution to Chap. 18..... | 478 |
| 19 | Hermitian Spaces | 481 |
| 19.1 | Hermitian Geometry..... | 481 |
| 19.1.1 | Gramians..... | 482 |
| 19.1.2 | Gram–Schmidt Orthogonalization Procedure..... | 482 |
| 19.1.3 | Cauchy–Schwarz Inequality..... | 483 |
| 19.1.4 | Unitary Group..... | 483 |

| | | |
|-----------|--|------------|
| 19.1.5 | Hermitian Volume | 484 |
| 19.1.6 | Hermitian Correlation | 484 |
| 19.1.7 | Orthogonal Projections | 485 |
| 19.1.8 | Angle Between Two Lines | 486 |
| 19.2 | Adjoint Linear Maps | 487 |
| 19.2.1 | Hermitian Adjunction | 487 |
| 19.2.2 | Adjoint Endomorphisms | 488 |
| 19.2.3 | Euclidean Adjunction | 489 |
| 19.3 | Normal Operators | 491 |
| 19.3.1 | Orthogonal Diagonalization | 491 |
| 19.3.2 | Normal Operators in Euclidean Space | 492 |
| 19.4 | Polar and Singular Value Decompositions | 495 |
| 19.4.1 | Polar Decomposition | 495 |
| 19.4.2 | Exponential Cover of the Unitary Group | 496 |
| 19.4.3 | Singular Value Decomposition | 497 |
| | Problems for Independent Solution to Chap. 19 | 499 |
| 20 | Quaternions and Spinors | 503 |
| 20.1 | Complex 2×2 Matrices and Quaternions | 503 |
| 20.1.1 | $\text{Mat}_2(\mathbb{C})$ as the Complexification of Euclidean \mathbb{R}^4 | 503 |
| 20.1.2 | Algebra of Quaternions | 505 |
| 20.1.3 | Real and Pure Imaginary Quaternions | 506 |
| 20.1.4 | Quaternionic Norm | 506 |
| 20.1.5 | Division | 507 |
| 20.2 | Geometry of Quaternions | 507 |
| 20.2.1 | Universal Covering $S^3 = \text{SU}_2 \rightarrow \text{SO}_3(\mathbb{R})$ | 509 |
| 20.2.2 | Topological Comment | 510 |
| 20.2.3 | Two Pencils of Hermitian Structures | 512 |
| 20.3 | Spinors | 513 |
| 20.3.1 | Geometry of Hermitian Enhancements of Euclidean \mathbb{R}^4 | 513 |
| 20.3.2 | Explicit Formulas | 514 |
| 20.3.3 | Hopf Bundle | 515 |
| | Problems for Independent Solution to Chap. 20 | 516 |
| | Hints to Selected Exercises | 519 |
| | References | 545 |
| | Index | 547 |

Notation and Abbreviations

| | |
|--|---|
| $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ | Positive integers, integers, rational numbers, real numbers, complex numbers, quaternions |
| \Rightarrow and \Longleftrightarrow | “implies” and “if and only if” |
| $\forall, \exists, :$ | “for all,” “there exists,” “such that” |
| $\text{Hom}(X, Y)$ | Set of maps or homomorphisms $X \rightarrow Y$ |
| $\text{End}(X) = \text{Hom}(X, X)$ | Set of maps or endomorphisms $X \rightarrow X$ |
| $\text{Aut}(X) \subset \text{End}(X)$ | Group of invertible maps or automorphisms $X \rightarrow X$ |
| $ M , G , \lambda $ | Cardinality of finite set M or group G , total number of cells in Young diagram λ |
| $ pq , v , \ v\ $ | Distance between points p, q and length (or norm) of vector v |
| $a:b$ (or $b \mid a$) | a is divisible by b (or b divides a) |
| $a \equiv b \pmod{n}$ | a is congruent to b modulo n (i.e., $(a - b):n$) |
| $\mathbb{Z}/(n), \mathbb{F}_q$ | Ring or additive group of integers modulo n , finite field of q elements |
| GCD, LCM, poset | Greatest common divisor, least common multiple, partially ordered set |
| S_n | The symmetric group $\text{Aut}\{1, 2, \dots, n\}$ |
| $(\sigma_1, \sigma_2, \dots, \sigma_n) \in S_n$ | Permutation $k \mapsto \sigma_k$ |
| $ i_1, i_2, \dots, i_m) \in S_n$ | Cyclic permutation $i_1 \mapsto i_2 \mapsto \dots \mapsto i_m \mapsto i_1$ |
| $K[x]$ and $K[[x]]$ | Rings of polynomials and formal power series with coefficients in commutative ring K |
| $\mathbb{k}[x_1, x_2, \dots, x_n]_{\leq m}$ | Vector space of polynomials of degree at most m in variables x_1, x_2, \dots, x_n with coefficients in field \mathbb{k} |
| $\mathbb{k}\langle \xi_1, \xi_2, \dots, \xi_n \rangle$ | Ring of Grassmannian polynomials in (skew commuting) variables $\xi_1, \xi_2, \dots, \xi_n$ |
| \mathbb{F}^*, K^* | Multiplicative groups of nonzero elements in field \mathbb{F} and of invertible elements in ring K |

| | |
|---|--|
| V^*, F^* | Dual vector space for vector space V and dual linear map for linear map F |
| ${}^\vee F, F^\vee, F^\dagger$ | Left and right adjoint operators for F with respect to nondegenerate bilinear form, and Hermitian adjoint operator for F |
| $\text{Mat}_{m \times n}(K), \text{Mat}_n(K)$ | Module of matrices having m rows and n columns, and K -algebra of square $n \times n$ matrices with elements in ring K |
| M^t, λ^t | Transposed matrix or Young diagram |
| $\langle \xi, v \rangle = \xi(v) = \text{ev}_v(\xi)$ | Contraction between vector $v \in V$ and covector $\xi \in V^*$ |
| (v, w) | Euclidean or Hermitian inner product of vectors v, w |
| $\mathbb{A}(V), \mathbb{P}(V)$ | Affine and projective spaces associated with a vector space V |
| $Z(f) \subset \mathbb{P}(V)$ | Hypersurface defined by equation $f(v) = 0$ |
| $\text{GL}(V), \text{O}(V), \text{U}(V), \text{PGL}(V)$ | Groups of linear, orthogonal, unitary transformations of a vector space V , and projective transformations of its projectivization $\mathbb{P}(V)$ |
| $\text{SL}(V), \text{SO}(V), \text{SU}(V)$ | Groups of linear, orthogonal, and unitary transformations of determinant 1 |
| $\text{GL}_n(\mathbb{k}), \text{PGL}_n(\mathbb{k}), \text{SL}_n(\mathbb{k}), \text{etc.}$ | Groups of $n \times n$ matrices obtained from the previous groups for $V = \mathbb{k}^n$ |
| $S^n V^*$ | Vector space of homogeneous degree- n polynomials on vector space V |
| Q, q, \tilde{q}, \hat{q} | Quadric $Q = Z(q) \subset \mathbb{P}(V)$ defined by equation $q(v) = 0$, where $q \in S^2 V^*$ has polarization $\tilde{q} : V \times V \rightarrow \mathbb{F}$ and correlation map $\hat{q} : V \rightarrow V^*$ |

Chapter 1

Set-Theoretic and Combinatorial Background

1.1 Sets and Maps

1.1.1 Sets

I have no desire to include a rigorous introduction to the theory of sets in this book. Perhaps what follows will motivate the interested reader to learn this theory in a special course on mathematical logic. In any case, the common intuitive understanding of a set as an abstract “aggregate of elements” is enough for our purposes. Any set can be imagined geometrically as a collection of points, and we will often refer to the elements of a set as points. By definition, all the elements of a set are distinct. A set X may be considered as having been adequately defined as soon as one can say that a given item is or is not an element of X . If x is an element of a set X , we write $x \in X$. Two sets are *equal* if they consist of the same elements. There is a unique set containing no elements. It is called the *empty set* and is denoted by \emptyset . For a finite set X , we write $|X|$ for the total number of elements in X and call it the *cardinality* of X . A set X is called a *subset* of a set Y if each element $x \in X$ also belongs to Y . In this case, we write $X \subset Y$. Note that \emptyset is a subset of every set, and every set is a subset of itself. A subset of a set X that is not equal to X is said to be *proper*.

Exercise 1.1 How many subsets (including the set itself) are there in a finite set of cardinality n ?

Given two sets X and Y , the *union* $X \cup Y$ consists of all elements belonging to at least one of them. The union of nonintersecting sets Y, Z is denoted by $Y \sqcup Z$ and called their *disjoint union*. The *intersection* $X \cap Y$ consists of all elements belonging to both sets X, Y simultaneously. The *set difference* $X \setminus Y$ consists of all elements

that belong to X but not to Y . The *direct product*¹ $X \times Y$ consists of all ordered pairs (x, y) , where $x \in X, y \in Y$.

Exercise 1.2 Check that the intersection can be expressed in terms of the difference as $X \cap Y = X \setminus (X \setminus Y)$. Is it possible to express the difference in terms of the intersection and union?

1.1.2 Maps

A *map* (or *function*) $f : X \rightarrow Y$ from a set X to a set Y is an assignment $x \mapsto f(x)$ that relates each point $x \in X$ with some point $y = f(x) \in Y$ called the *image* of x under f or the *value* of f at x . Note that y must be uniquely determined by x and f . Two maps $f : X \rightarrow Y$ and $g : X \rightarrow Y$ are said to be *equal* if $f(x) = g(x)$ for all $x \in X$. We write $\text{Hom}(X, Y)$ for the set of all maps $X \rightarrow Y$.

All points $x \in X$ sent by the map $f : X \rightarrow Y$ to a given point $y \in Y$ form a subset of X denoted by

$$f^{-1}(y) \stackrel{\text{def}}{=} \{x \in X \mid f(x) = y\}$$

and called the *preimage* of y under f or the *fiber* of f over y . The preimages of distinct points are disjoint and may consist of arbitrarily many points or even be empty. The points $y \in Y$ with a nonempty preimage form a subset of Y called the *image* of f and denoted by

$$\text{im}(f) \stackrel{\text{def}}{=} \{y \in Y \mid f^{-1}(y) \neq \emptyset\} = \{y \in Y \mid \exists x \in X : f(x) = y\}.$$

A map $f : X \rightarrow Y$ is called *surjective* (or an *epimorphism*) if the preimage of every point $y \in Y$ is nonempty, i.e., if $\text{im}(f) = Y$. We designate a surjective map by a two-headed arrow $X \twoheadrightarrow Y$. A map f is called *injective* (or a *monomorphism*) if the preimage of every point $y \in Y$ contains at most one element, i.e., $f(x_1) \neq f(x_2)$ for all $x_1 \neq x_2$. Injective maps are designated by a hooked arrow $X \hookrightarrow Y$.

Exercise 1.3 List all maps $\{0, 1, 2\} \rightarrow \{0, 1\}$ and all maps $\{0, 1\} \rightarrow \{0, 1, 2\}$. How many epimorphisms and monomorphisms are there among them in each case?

A map $f : X \rightarrow Y$ is called *bijective* or an *isomorphism* if it is simultaneously surjective and injective. This means that for every $y \in Y$, there exists a unique $x \in X$ such that $f(x) = y$. For this reason, a bijection is also called a *one-to-one*

¹Also called the *Cartesian product* of sets.

correspondence between X and Y . We designate a bijection by an arrow with a tilde over it: $X \simeq Y$.

Exercise 1.4 Indicate all bijections, injections, and surjections among the following maps: **(a)** $\mathbb{N} \rightarrow \mathbb{N}, x \mapsto x^2$, **(b)** $\mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto x^2$, **(c)** $\mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto 7x$, **(d)** $\mathbb{Q} \rightarrow \mathbb{Q}, x \mapsto 7x$.

A map from X to itself is called an *endomorphism* of X . We write $\text{End}(X) \stackrel{\text{def}}{=} \text{Hom}(X, X)$ for the set of all endomorphisms of X . Bijective endomorphisms $X \simeq X$ are called *automorphisms* of X . We denote the set of all automorphisms by $\text{Aut}(X)$. One can think of an automorphism $X \simeq X$ as a permutation of the elements of X . The trivial permutation $\text{Id}_X : X \rightarrow X, x \mapsto x$, which takes each element to itself, is called the *identity map*.

Exercise 1.5 (Dirichlet's Principle) Convince yourself that the following conditions on a set X are equivalent: **(a)** X is infinite; **(b)** there exists a nonsurjective injection $X \hookrightarrow X$; **(c)** there exists a noninjective surjection $X \twoheadrightarrow X$.

Exercise 1.6 Show that $\text{Aut}(\mathbb{N})$ is an uncountable set.²

Example 1.1 (Recording Maps by Words) Given two finite sets $X = \{1, 2, \dots, n\}$, $Y = \{1, 2, \dots, m\}$, every map $f : X \rightarrow Y$ can be represented by a sequence of its values $w(f) \stackrel{\text{def}}{=} (f(1), f(2), \dots, f(n))$ viewed as an n -letter word in the m -letter alphabet Y . For example, the maps $f : \{1, 2\} \rightarrow \{1, 2, 3\}$ and $g : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ defined by the assignments $f(1) = 3, f(2) = 2$ and $g(1) = 1, g(2) = 2, g(3) = 2$ are represented by the words $w(f) = (3, 2)$ and $w(g) = (1, 2, 2)$ in the alphabet $\{1, 2, 3\}$. Therefore, we get the bijection

$$w : \text{Hom}(X, Y) \simeq \{|X| - \text{letter words in the alphabet } Y\}, \quad f \mapsto w(f).$$

This map takes monomorphisms to words without duplicate letters. Epimorphisms go to words containing the whole alphabet. Isomorphisms go to words in which every letter of the alphabet appears exactly once.

1.1.3 Fibers of Maps

A map $f : X \rightarrow Y$ decomposes X into the disjoint union of nonempty subsets $f^{-1}(y)$ indexed by the elements $y \in \text{im}(f)$:

$$X = \bigsqcup_{y \in \text{im}(f)} f^{-1}(y). \quad (1.1)$$

²A set is called *countable* if it is isomorphic to \mathbb{N} . An infinite set not isomorphic to \mathbb{N} is called *uncountable*.

This viewpoint may be useful when we need to compare cardinalities of sets. For example, if all fibers of the map $f : X \rightarrow Y$ have the same cardinality $m = |f^{-1}(y)|$, then

$$|X| = m \cdot |\operatorname{im} f|. \quad (1.2)$$

Proposition 1.1 $|\operatorname{Hom}(X, Y)| = |Y|^{|X|}$ for all finite sets X, Y .

Proof Fix an arbitrary point $x \in X$ and consider the evaluation map

$$\operatorname{ev}_x : \operatorname{Hom}(X, Y) \rightarrow Y, \quad f \mapsto f(x), \quad (1.3)$$

which takes the map $f : X \rightarrow Y$ to its value at x . The maps $X \rightarrow Y$ with a prescribed value at x are in bijection with the maps $X \setminus \{x\} \rightarrow Y$. Thus, $|\operatorname{ev}_x^{-1}(y)| = |\operatorname{Hom}(X \setminus \{x\}, Y)|$ for all $y \in Y$. Hence, $|\operatorname{Hom}(X, Y)| = |\operatorname{Hom}(X \setminus \{x\}, Y)| \cdot |Y|$ by formula (1.2). In other words, when we add one more point to X , the cardinality of $\operatorname{Hom}(X, Y)$ is multiplied by $|Y|$. \square

Remark 1.1 In the light of Proposition 1.1, the set of all maps $X \rightarrow Y$ is often denoted by

$$Y^X \stackrel{\text{def}}{=} \operatorname{Hom}(X, Y).$$

Remark 1.2 In the above proof, we assumed that both sets are nonempty. If $X = \emptyset$, then for each Y , there exists just one map $\emptyset \hookrightarrow Y$, namely the empty map, which takes every element of X (of which there are none) to an arbitrary element of Y . In this case, the evaluation map (1.3) is not defined. However, Proposition 1.1 is still true: $1 = |Y|^0$. Note that $\operatorname{Hom}(\emptyset, \emptyset) = \{\operatorname{Id}_\emptyset\}$ has cardinality 1, i.e., $0^0 = 1$ in our current context. If $Y = \emptyset$, then $\operatorname{Hom}(X, \emptyset) = \emptyset$ for every $X \neq \emptyset$. This agrees with Proposition 1.1 as well: $0^{|X|} = 0$ for $|X| > 0$.

Proposition 1.2 Let $|X| = |Y| = n$. We write $\operatorname{Isom}(X, Y) \subset \operatorname{Hom}(X, Y)$ for the set of all bijections $X \xrightarrow{\sim} Y$. Then $|\operatorname{Isom}(X, Y)| = n!$, where $n! \stackrel{\text{def}}{=} n \cdot (n-1) \cdot (n-2) \cdots 1$. In particular, $|\operatorname{Aut}(X)| = n!$.

Proof For every $x \in X$, the restriction of the evaluation map (1.3) to the subset of bijections assigns the surjective map $\operatorname{ev}_x : \operatorname{Isom}(X, Y) \twoheadrightarrow Y, f \mapsto f(x)$. The bijections $f : X \xrightarrow{\sim} Y$ with a prescribed value $y = f(x)$ are in one-to-one correspondence with all bijections $X \setminus \{x\} \rightarrow Y \setminus \{y\}$. Since the cardinality of $\operatorname{Isom}(X \setminus \{x\}, Y \setminus \{y\})$ does not depend on x, y , we have $|\operatorname{Isom}(X, Y)| = |\operatorname{Isom}(X \setminus \{x\}, Y \setminus \{y\})| \cdot |Y|$ by formula (1.2). In other words, when we add one more point to both X and Y , the cardinality of $\operatorname{Isom}(X, Y)$ is multiplied by $|Y| + 1$. \square

Remark 1.3 The product $n! = n \cdot (n-1) \cdot (n-2) \cdots 1$ is called *n-factorial*. Since $\operatorname{Aut}(\emptyset) = \{\operatorname{Id}_\emptyset\}$ has cardinality 1, we define $0! \stackrel{\text{def}}{=} 1$.

Example 1.2 (Multinomial Coefficients) To multiply out the expression $(a_1 + a_2 + \cdots + a_m)^n$, we may place the factors in a line:

$$(a_1 + a_2 + \cdots + a_m) \cdot (a_1 + a_2 + \cdots + a_m) \cdots (a_1 + a_2 + \cdots + a_m).$$

Then for each $i = 1, 2, \dots, n$, we choose some letter a_{v_i} within the i th pair of parentheses and form the word $a_{v_1}a_{v_2} \dots a_{v_n}$ from them. After doing this in all possible ways, adding all the words together, and collecting like monomials, we get the sum

$$(a_1 + a_2 + \cdots + a_m)^n = \sum_{\substack{k_1+k_2+\dots+k_m=n \\ \forall i, 0 \leq k_i \leq n}} \binom{n}{k_1, \dots, k_m} \cdot a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}, \quad (1.4)$$

where each exponent k_i varies over the range $0 \leq k_i \leq n$, and the total degree of each monomial is equal to $n = k_1 + k_2 + \cdots + k_m$. The coefficient $\binom{n}{k_1, \dots, k_m}$ of the monomial $a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$ is called a *multinomial coefficient*. It equals the number of all n -letter words that can be written with exactly k_1 letters a_1 , k_2 letters a_2 , etc. To evaluate it precisely, write Y for the set of all such words. Then for each $i = 1, 2, \dots, n$, mark the k_i identical letters a_i each with different upper index $1, 2, \dots, k_i$ in order to distinguish these letters from one another. Now write X for the set of all n -letter words written with n distinct marked letters

$$\underbrace{a_1^{(1)}, a_1^{(2)}, \dots, a_1^{(k_1)}}_{k_1 \text{ marked letters } a_1}, \underbrace{a_2^{(1)}, a_2^{(2)}, \dots, a_2^{(k_2)}}_{k_2 \text{ marked letters } a_2}, \dots, \underbrace{a_m^{(1)}, a_m^{(2)}, \dots, a_m^{(k_m)}}_{k_m \text{ marked letters } a_m}$$

and containing each letter exactly once. We know from Proposition 1.2 that $|X| = n!$. Consider the *forgetful surjection* $f : X \twoheadrightarrow Y$, which erases all the upper indices. The preimage of every word $y \in Y$ under this map consists of the $k_1! \cdot k_2! \cdots k_m!$ words obtained from y by marking the k_1 letters a_1 , k_2 letters a_2 , etc. with upper indices in all possible ways. (1.2) on p. 4 leads to

$$\binom{n}{k_1, \dots, k_m} = \frac{n!}{k_1! \cdot k_2! \cdots k_m!}. \quad (1.5)$$

Thus, the expansion (1.4) becomes

$$(a_1 + a_2 + \cdots + a_m)^n = \sum_{\substack{k_1+\dots+k_m=n \\ \forall i, 0 \leq k_i \leq n}} \frac{n! \cdot a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}}{k_1! \cdot k_2! \cdots k_m!}. \quad (1.6)$$

Exercise 1.7 How many summands are there on the right-hand side of (1.6)?

For $m = 2$, we get the following well-known formula³:

$$(a + b)^n = \sum_{k=0}^n \frac{n! \cdot a^k b^{n-k}}{k!(n-k)!}. \quad (1.7)$$

The *binomial coefficient* $\frac{n!}{k!(n-k)!}$ is usually denoted by either $\binom{n}{k}$ or C_n^k instead of $\binom{n}{k, n-k}$. We will use the notation $\binom{n}{k}$. Note that it can be written as

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k \cdot (k-1) \cdots 1},$$

where both the numerator and denominator consist of k decreasing integer factors.

Example 1.3 (Young Diagrams) The decomposition of the finite set $X = \{1, 2, \dots, n\}$ into a disjoint union of nonempty subsets

$$X = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_k \quad (1.8)$$

can be encoded as follows. Renumber the subsets X_i in any nonincreasing order of their cardinalities and set $\lambda_i = |X_i|$. We obtain a nonincreasing sequence of integers

$$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n), \quad \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k, \quad (1.9)$$

called a *partition* of $n = |X|$ or a *shape* of the decomposition (1.8). Partitions are visualized by diagrams like this:


(1.10)

Such a diagram is formed by cellular strips of lengths $\lambda_1, \lambda_2, \dots, \lambda_k$ aligned at the left and of nonincreasing length from top to bottom. It is called a *Young diagram* of the partition λ . We will make no distinction between a partition and its diagram and denote both by the same letter. The total number of cells in the diagram λ is called the *weight* and denoted by $|\lambda|$. The number of rows is called the *length* of the

³This is a particular case of the generic *Newton's binomial theorem*, which expands $(1+x)^s$ with an arbitrary α . We will prove it in Sect. 1.2.

diagram and denoted by $\ell(\lambda)$. Thus, the Young diagram (1.10) depicts the partition $\lambda = (6, 5, 5, 3, 1)$ of weight $|\lambda| = 20$ and length $\ell(\lambda) = 5$.

Exercise 1.8 How many Young diagrams can be drawn within a $k \times n$ rectangle?⁴

If we fill the cells of λ by the elements of X (one element per cell) and combine the elements placed in row i into one subset $X_i \subset X$, then we obtain the decomposition (1.8) of shape λ . Since every decomposition of shape λ can be achieved in this way from an appropriate filling, we get a surjective map from the set of all fillings of λ to the set of all decompositions (1.8) of shape λ . All the fibers of this map have the same cardinality. Namely, two fillings produce the same decomposition if and only if they are obtained from each other either by permuting elements within rows or by permuting entire rows of equal length. Let us write m_i for the number of rows of length⁵ i in λ . By Proposition 1.2, there are $\prod \lambda_i! = \prod_{i=1}^n (i!)^{m_i}$ permutations of the first type and $\prod_{i=1}^n m_i!$ permutations of the second type. Since they act independently, each fiber has cardinality $\prod_{i=1}^n (i!)^{m_i} m_i!$. Therefore, $n!$ fillings produce

$$\frac{n!}{\prod_{i=1}^n m_i! \cdot (i!)^{m_i}} \quad (1.11)$$

different decompositions of a set of cardinality n into a disjoint union of m_1 elements, m_2 subsets of cardinality 2, m_3 subsets of cardinality 3, etc.

1.2 Equivalence Classes

1.2.1 Equivalence Relations

Another way of decomposing X into a disjoint union of subsets is to declare the elements in each subset to be *equivalent*. This can be formalized as follows. A subset $R \subset X \times X = \{(x_1, x_2) \mid x_1, x_2 \in X\}$ is called a *binary relation* on X . If $(x_1, x_2) \in R$, we write $x_1 \sim_R x_2$ and say that R relates x_1 with x_2 . We omit the letter R from this notation when R is clear from context or is inessential.

For example, the following binary relations on the set of integers \mathbb{Z} are commonly used:

$$\text{equality} : x_1 \sim x_2, \text{ meaning that } x_1 = x_2; \quad (1.12)$$

$$\text{inequality} : x_1 \sim x_2, \text{ meaning that } x_1 \leq x_2; \quad (1.13)$$

⁴The upper left-hand corner of each diagram should coincide with that of the rectangle. The empty diagram and the whole rectangle are allowed.

⁵Note that the equality $|\lambda| = n = m_1 + 2m_2 + \cdots + nm_n$ forces many of the m_i to vanish.

divisibility : $x_1 \sim x_2$, meaning that $x_1 \mid x_2$; (1.14)

congruence modulo n : $x_1 \sim x_2$, meaning that $x_1 \equiv x_2 \pmod{n}$. (1.15)

(The last of these is read “ x_1 is congruent to x_2 modulo n ” and signifies that n divides $x_1 - x_2$.)

Definition 1.1 A binary relation \sim is called an *equivalence relation* or simply an *equivalence* if it satisfies the following three properties:

$$\begin{aligned} \text{reflexivity: } & \forall x \in X, \quad x \sim x; \\ \text{transitivity: } & \forall x_1, x_2, x_3 \in X, \quad x_1 \sim x_2 \ \& \ x_2 \sim x_3 \implies x_1 \sim x_3; \\ \text{symmetry: } & \forall x_1, x_2 \in X, \quad x_1 \sim x_2 \iff x_2 \sim x_1. \end{aligned}$$

In the above list of binary relations on \mathbb{Z} , (1.12) and (1.15) are equivalences. Relations (1.13) and (1.14) are not symmetric.⁶

If X is decomposed into a disjoint union of subsets, then the relation $x_1 \sim x_2$, meaning that x_1, x_2 belong to the same subset, is an equivalence relation. Conversely, given an equivalence relation R on X , let us introduce the notion of an *equivalence class* of x as

$$[x]_R \stackrel{\text{def}}{=} \{z \in X \mid x \sim_R z\} = \{z \in X \mid z \sim_R x\},$$

where the second equality holds because R is symmetric.

Exercise 1.9 Verify that any two classes $[x]_R, [y]_R$ either coincide or are disjoint.

Thus, X decomposes into a disjoint union of distinct equivalence classes. The set of these equivalence classes is denoted by X/R and called the *quotient* or *factor set* of X by R . The surjective map sending an element to its equivalence class,

$$f : X \twoheadrightarrow X/R, \quad x \mapsto [x]_R, \quad (1.16)$$

is called the *quotient map* or *factorization map*. Its fibers are exactly the equivalence classes. Every surjective map $f : X \twoheadrightarrow Y$ is the quotient map modulo the equivalence defined by $x_1 \sim x_2$ if $f(x_1) = f(x_2)$.

Example 1.4 (Residue Classes) Fix a nonzero $n \in \mathbb{Z}$ and write $\mathbb{Z}/(n)$ for the quotient of \mathbb{Z} modulo the congruence relation (1.15). The elements of $\mathbb{Z}/(n)$ are called *residue classes modulo n* . The class of a number $z \in \mathbb{Z}$ is denoted by $[z]_n$ or simply by $[z]$ when the value of n is clear from context or is inessential.

⁶They are *skew-symmetric*, i.e., they satisfy the condition $x_1 \sim x_2 \ \& \ x_2 \sim x_1 \implies x_1 = x_2$; see Sect. 1.4 on p. 13.

The factorization map

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n), \quad z \mapsto [z]_n,$$

is called *reduction modulo n* . The set $\mathbb{Z}/(n)$ consists of the n elements $[0]_n, [1]_n, \dots, [n-1]_n$, in bijection with the residues of division by n . However, it may sometimes be more productive to think of residue classes as subsets in \mathbb{Z} , because this allows us to vary the representation of an element depending on what we need. For example, the residue of division of 12^{100} by 13 can be evaluated promptly as follows:

$$[12^{100}]_{13} = [12]_{13}^{100} = [-1]_{13}^{100} = [(-1)^{100}]_{13} = [1]_{13}.$$

Exercise 1.10 Prove the consistency of the above computation, i.e., verify that the residue classes $[x+y]_n$ and $[xy]_n$ do not depend on the choice of elements $x \in [x]_n$ and $y \in [y]_n$ used in their representations.

Thus, the quotient set $\mathbb{Z}/(n)$ has a well-defined addition and multiplication given by

$$[x]_n + [y]_n \stackrel{\text{def}}{=} [x+y]_n, \quad [x]_n \cdot [y]_n \stackrel{\text{def}}{=} [xy]_n. \quad (1.17)$$

1.2.2 Implicitly Defined Equivalences

Given a family of equivalence relations $R_v \subset X \times X$, the intersection $\bigcap R_v \subset X \times X$ is again an equivalence relation. Indeed, if each set $R_v \subset X \times X$ contains the diagonal $\Delta = \{(x, x) \mid x \in X\} \subset X \times X$ (reflexivity), goes to itself under reflection $(x_1, x_2) \rightleftharpoons (x_2, x_1)$ (symmetry), and contains for every pair of points $(x, y), (y, z) \in R_v$ the point (x, z) as well (transitivity), then the intersection $\bigcap R_v$ will inherit the same properties. Therefore, for every subset $S \subset X \times X$, there exists a unique equivalence relation $\bar{S} \supset S$ contained in all equivalence relations containing S . It is called the equivalence relation *generated* by S and can be described as the intersection of all equivalence relations containing S . A more constructive description is given in the next exercise.

Exercise 1.11 Check that x is related to y by \bar{R} if and only if there exists a finite sequence of points $x = z_0, z_1, z_2, \dots, z_n = y$ in X such that for each $i = 1, 2, \dots, n$, either (x_{i-1}, x_i) or (x_i, x_{i-1}) belongs to R .

However, such an implicit description may be quite ineffective even for understanding whether there are any inequivalent points at all.

Example 1.5 (Fractions) The set of rational numbers \mathbb{Q} is usually introduced as the set of *fractions* a/b , where $a, b \in \mathbb{Z}$, $b \neq 0$. By definition, such a fraction is an equivalence class of the pair $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus 0)$ modulo the equivalence generated

by the relations

$$(a, b) \sim (ac, bc) \quad \text{for all } c \in \mathbb{Z} \setminus 0, \quad (1.18)$$

which assert the equality of the fractions $a/b = (ac)/(bc)$. The relations (1.18) do not themselves form an equivalence relation. Indeed, if $a_1b_2 = a_2b_1$, then the leftmost element in the two-step chain

$$(a_1, b_1) \sim (a_1b_2, b_1b_2) = (a_2b_1, b_1b_2) \sim (a_2, b_2)$$

may not be related to the rightmost one directly by (1.18). For example, $3/6$ and $5/10$ produce equal fractions and are not directly related. Thus, the equivalence generated by (1.18) must contain the relations

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{for all } a_1b_2 = a_2b_1. \quad (1.19)$$

Exercise 1.12 Verify that the relations (1.19) are reflexive, symmetric, and transitive.

Hence, relations (1.19) give a complete explicit description for the equivalence generated by relations (1.18).

1.3 Compositions of Maps

1.3.1 Composition Versus Multiplication

A *composition* of maps $F : X \rightarrow Y$ and $g : Y \rightarrow Z$ is a map

$$g \circ f : X \rightarrow Z, \quad x \mapsto g(f(x)).$$

The notation $g \circ f$ is usually shorted to gf , which should not be confused with a product of numbers. In fact, the algebraic properties of compositions differ from those used in numeric computations. The composition of maps is not commutative: $fg \neq gf$ in general. When fg is defined, gf may not be. Even if both compositions are well defined, say for endomorphisms $f, g \in \text{End}(X)$ of some set X , the equality $fg = gf$ usually fails.

Exercise 1.13 Let two lines ℓ_1, ℓ_2 in the plane cross at the point O . Write σ_1 and σ_2 for the reflections (i.e., axial symmetries) of the plane in these lines. Describe explicitly the motions $\sigma_1\sigma_2$ and $\sigma_2\sigma_1$. How should the lines be situated in order to get $\sigma_1\sigma_2 = \sigma_2\sigma_1$?

Cancellation of common factors also fails. Generically, neither $fg = fh$ nor $gf = hf$ implies $g = h$.

Example 1.6 (Endomorphisms of a Two-Element Set) The set $X = \{1, 2\}$ has four endomorphisms. Let us record maps $f : X \rightarrow X$ by two-letter words $(f(1), f(2))$ as in Example 1.1 on p. 3. Then the four endomorphisms X are $(1, 1), (1, 2) = \text{Id}_X, (2, 1), (2, 2)$. The compositions fg are collected in the following multiplication table:

$$\begin{array}{c|cccc}
 f \backslash g & (1, 1) & (1, 2) & (2, 1) & (2, 2) \\
 \hline
 (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\
 (1, 2) & (1, 1) & (1, 2) & (2, 1) & (2, 2) \\
 (2, 1) & (2, 2) & (2, 1) & (1, 2) & (1, 1) \\
 (2, 2) & (2, 2) & (2, 2) & (2, 2) & (2, 2)
 \end{array} \tag{1.20}$$

Note that $(2, 2) \circ (1, 1) \neq (1, 1) \circ (2, 2)$, $(1, 1) \circ (1, 2) = (1, 1) \circ (2, 1)$, whereas $(1, 2) \neq (2, 1)$ and $(1, 1) \circ (2, 2) = (2, 1) \circ (2, 2)$, whereas $(1, 1) \neq (2, 1)$.

The only nice property of numeric multiplication shared by the composition of maps is *associativity*: $(hg)f = h(gf)$ for every triple of maps $f : X \rightarrow Y, g : Y \rightarrow Z, h : Z \rightarrow T$. Indeed, in each case, we have $x \mapsto h(g(f(x)))$.

Lemma 1.1 (Left Inverse Map) *The following conditions on a map $f : X \rightarrow Y$ are equivalent:*

1. f is injective;
2. there exists a map $g : Y \rightarrow X$ such that $gf = \text{Id}_X$ (any such g is called a *left inverse* to f);
3. for any two maps $g_1, g_2 : Y \rightarrow X$ such that $fg_1 = fg_2$, the equality $g_1 = g_2$ holds.

Proof We verify the implications $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1)$. Let f be injective. For $y = f(x)$, put $g(y) = x$. For $y \notin \text{im } f$, define $g(y)$ arbitrarily. Then $g : Y \rightarrow X$ satisfies (2). If (2) holds, then the left composition of both sides of the equality $fg_1 = fg_2$ with g leads to $g_1 = g_2$. Finally, if $f(x_1) = f(x_2)$ for some $x_1 \neq x_2$, then (3) is not satisfied for $g_1 = \text{Id}_X$ and $g_2 : X \rightarrow X$ that swaps x_1, x_2 and leaves all the other points fixed. \square

1.3.2 Right Inverse Map and the Axiom of Choice

A feeling of harmony calls for the right counterpart of Lemma 1.1. We expect that the following conditions on a map $f : X \rightarrow Y$ should be equivalent:

- (1) f is surjective;
- (2) there exists a map $g : Y \rightarrow X$ such that $fg = \text{Id}_Y$;
- (3) for any two maps $g_1, g_2 : Y \rightarrow X$ such that $g_1f = g_2f$, the equality $g_1 = g_2$ holds.

If these conditions hold, we shall call the map g from (2) a *right inverse* to f . Another conventional name for g is a *section* of the surjective map f , because every map g

satisfying (2) just selects some element $g(y) \in f^{-1}(y)$ in the fiber of f over each point $y \in Y$ simultaneously for all $y \in Y$. In rigorous set theory, which we try to avoid here, there is a special *selection axiom*, called the *axiom of choice*, postulating that every surjective map of sets admits a section. Thus, implication (1) \Rightarrow (2) is part of the rigorous definition of a set. The proof of the implication (2) \Rightarrow (3) is completely symmetric to the proof from Lemma 1.1: compose both sides of $g_1 f = g_2 f$ with g from the right and obtain $g_1 = g_2$. Implication (3) \Rightarrow (1) is proved by contradiction: if $y \notin \text{im } f$, then (1) fails for $g_1 = \text{Id}_Y$ and every $g_2 : Y \rightarrow Y$ that takes y to some point in $\text{im } f$ and leaves all other points fixed. Therefore, the above three properties, symmetric to those of Lemma 1.1, are equivalent as well.

1.3.3 Invertible Maps

If a map $f : X \rightarrow Y$ is bijective, then the preimage $f^{-1}(y) \subset X$ of a point $y \in Y$ consists of exactly one point. Therefore, the prescription $y \mapsto f^{-1}(y)$ defines a map $f^{-1} : Y \rightarrow X$ that is simultaneously a left and right inverse to f , i.e., it satisfies the equalities

$$f \circ f^{-1} = \text{Id}_Y \quad \text{and} \quad f^{-1} \circ f = \text{Id}_X. \quad (1.21)$$

The map f^{-1} is called a (*two-sided*) *inverse* to f .

Proposition 1.3 *The following properties of a map $f : X \rightarrow Y$ are equivalent:*

- (1) *f is bijective;*
- (2) *there exists a map $g : Y \rightarrow X$ such that $f \circ g = \text{Id}_Y$ and $g \circ f = \text{Id}_X$;*
- (3) *there exist maps $g', g'' : Y \rightarrow X$ such that $g' \circ f = \text{Id}_X$ and $f \circ g'' = \text{Id}_Y$.*

If f satisfies these properties, then $g = g' = g'' = f^{-1}$, where f^{-1} is the map defined before formula (1.21).

Proof If (1) holds, then $g = f^{-1}$ satisfies (2). Implication (2) \Rightarrow (3) is obvious. Conversely, if (3) holds, then $g' = g' \circ \text{Id}_Y = g' \circ (f \circ g'') = (g' \circ f) \circ g'' = \text{Id}_X \circ g'' = g''$. Therefore, (2) holds for $g = g' = g''$. Finally, let (2) hold. Then for every $y \in Y$, the preimage $f^{-1}(y)$ contains $g(y)$, because $f(g(y)) = y$. Moreover, every $x \in f^{-1}(y)$ equals $g(y)$: $x = \text{Id}_X(x) = g(f(x)) = g(y)$. Hence, f is bijective, and $g = f^{-1}$. \square

1.3.4 Transformation Groups

Let X be an arbitrary set. A nonempty subset $G \subset \text{Aut } X$ is called a *transformation group* of X if $\forall g_1, g_2 \in G, g_1 g_2 \in G$ and $\forall g \in G, g^{-1} \in G$. Note that every transformation group automatically contains the identity map Id_X , because $\text{Id}_X = g^{-1}g$ for every $g \in G$. For a finite transformation group G , its cardinality $|G|$ is

called the *order* of G . Every transformation group $H \subset G$ is called a *subgroup* of G . Every transformation group is a subgroup of the group $\text{Aut}(X)$ of all automorphisms of X .

Example 1.7 (Permutation Groups) For $X = \{1, 2, \dots, n\}$, the group $\text{Aut}(X)$ is denoted by S_n and called the *n*th *symmetric group* or the *permutation group* of n elements. By Proposition 1.2, $|S_n| = n!$. We will indicate a permutation $\sigma \in S_n$ by the row $(\sigma_1, \sigma_2, \dots, \sigma_n)$ of its values $\sigma_i = \sigma(i)$, as in Example 1.1. For example,

$$\sigma = (3, 4, 2, 1) \quad \text{and} \quad \tau = (2, 3, 4, 1)$$

encode the maps

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 2 & 1 \end{array} \quad \text{and} \quad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}$$

The compositions of these maps are recorded as $\sigma\tau = (4, 2, 1, 3)$ and $\tau\sigma = (4, 1, 3, 2)$.

Exercise 1.14 For the six elements of the symmetric group S_3 , write a multiplication table similar to that from formula (1.20) on p. 11.

Example 1.8 (Abelian Groups) A group G in which every two elements $f, g \in G$ commute, i.e., satisfy the relation $fg = gf$, is called *commutative* or *abelian*. Examples of abelian groups are the group T of parallel displacements of the Euclidean plane and the group SO_2 of the rotations of the plane about some fixed point. For every integer $n \geq 2$, rotations by integer multiples of $2\pi/n$ form a finite subgroup of SO_2 called the *cyclic group* of order n .

1.4 Posets

1.4.1 Partial Order Relations

A binary relation⁷ $x \leq y$ on a set Z is called a *partial order* if, like an equivalence relation, it is reflexive and transitive,⁸ but instead of symmetric, it is *skew-symmetric*, which means that $x \leq y$ and $y \leq x$ imply $x = y$. If some partial order is given, we

⁷See Sect. 1.2 on p. 7.

⁸See Definition 1.1 on p. 8.

write $x < y$ if $x \leq y$ and $x \neq y$. A partial order on Z is called a *total order* if for all $x, y \in Z$, $x < y$ or $x = y$ or $y < x$ holds. For example, the usual inequality of numbers provides the set of integers \mathbb{Z} with a total order, whereas the divisibility relation $n \mid m$, meaning that n divides m , is a partial but not total order on \mathbb{Z} . Another important example of a nontotal partial order is the one provided by inclusions on the set $\mathcal{S}(X)$ of all subsets in a given set X .

Exercise 1.15 (Preorder) Let a set Z be equipped with a reflexive transitive binary relation⁹ $x \lesssim y$. We write $x \sim y$ if both $x \lesssim y$ and $y \lesssim x$ hold simultaneously. Verify that \sim is an equivalence relation and that on the quotient set Z/\sim , a partial order is well defined by the rule $[x] \leq [y]$ if $x \lesssim y$.

A set P equipped with a partial order is called a *partially ordered set*, or *poset* for short. If the order is total, we say that P is totally ordered. Every subset X of a poset P is certainly a poset with respect to the order on P . Totally ordered subsets of a poset P are called *chains*. Elements $x, y \in Z$ are called *incompatible* if neither $x \leq y$ nor $y \leq x$ holds. Otherwise, x, y are said to be *compatible*. Thus, a partial order is total if and only if every two elements are compatible. Note that two incompatible elements have to be distinct.

A map $f : M \rightarrow N$ between two posets is called *order-preserving*¹⁰ if for all $x, y \in M$, the inequality $x \leq y$ implies the inequality $f(x) \leq f(y)$. Posets M, N are said to be *isomorphic* if there is an order-preserving bijection $M \simeq N$. We write $M \simeq N$ in this case. A map f is called *strictly increasing* if for all $x, y \in M$, the inequality $x < y$ implies the inequality $f(x) < f(y)$. Every injective order-preserving map is strictly increasing. The converse is true for maps with totally ordered domain and may fail in general.

An element $y \in P$ is called an *upper bound* for a subset $X \subset P$ if $x \leq y$ for all $x \in X$. Such an upper bound is called *exterior* if $y \notin X$. In this case, the strong inequality $x < y$ holds for all $x \in X$.

An element $m^* \in X$ is called *maximal* in X if for all $x \in X$, the inequality $m^* \leq x$ implies $x = m^*$. Note that such an element may be incompatible with some $x \in X$, and therefore it is not necessarily an upper bound for X . A poset may have many different maximal elements or may not have any, like the poset \mathbb{Z} . If X is totally ordered, then the existence of a maximal element forces such an element to be unique. *Minimal elements* are defined symmetrically: $m_* \in X$ is called *minimal* if $\forall x \in X, m_* \leq x \Rightarrow x = m_*$, and the above discussion for maximal elements carries over to minimal elements with the obvious changes.

⁹Every such relation is called a *partial preorder* on \mathbb{Z} .

¹⁰Also *nondecreasing* or *nonstrictly increasing* or a *homomorphism of posets*.

1.4.2 Well-Ordered Sets

A totally ordered set W is called *well ordered* if every subset $U \subset W$ has a minimal element.¹¹ For example, the set \mathbb{N} of positive integers is well ordered by the usual inequality between numbers. All well-ordered sets share one of the most important properties of the positive integers: they allow proofs by induction. If some statement $\Sigma = \Sigma(w)$ depends on an element w running through a well-ordered set W , then $\Sigma(w)$ holds for all $w \in W$ as soon as the following two statements are proven:

- (1) $\Sigma(w_*)$ holds for the minimal element w_* of W ;
- (2) for every $x \in W$, if $\Sigma(w)$ holds for all $w < x$, then $\Sigma(x)$ holds.

This is known as the *principle of transfinite induction*.

Exercise 1.16 Verify the principle of transfinite induction.

Let us write $[y] \stackrel{\text{def}}{=} \{w \in W \mid w < y\}$ for the set of all elements strictly preceding y in a well-ordered set W and call it the *initial segment* of W preceding y . Note that y is uniquely determined by $[y]$ as the minimal element in $W \setminus [y]$. For the minimal element w_* of the whole of W , we set $[w_*] \stackrel{\text{def}}{=} \emptyset$. We write $U \leq W$ if $U \simeq [w]$ for some $w \in W$, and write $U < W$ if $U \leq W$ and $U \not\simeq W$. As good training in the use of the principle of transfinite induction, I strongly recommend the following exercise.

Exercise 1.17 For any two well ordered sets U, W , either $U < W$ or $U \simeq W$ or $W < U$ holds.

Classes of isomorphic well-ordered sets are called *cardinals*. Thus, the set \mathbb{N} can be identified with the set of all finite cardinals. All the other cardinals, including \mathbb{N} itself, are called *transfinite*.

1.4.3 Zorn's Lemma

Let P be a poset. We write $\mathcal{W}(P)$ for the set of all well-ordered (by the partial order on P) subsets $W \subset P$. Certainly, $\mathcal{W}(P) \neq \emptyset$, because all one-point subsets of P are within $\mathcal{W}(P)$. We also include \emptyset as an element of $\mathcal{W}(P)$.

Lemma 1.2 *For every poset P , there is no map $\beta : \mathcal{W}(P) \rightarrow P$ sending each $W \in \mathcal{W}(P)$ to some exterior upper bound of W .*

Proof Let such a map β exist. We will say that $W \in \mathcal{W}(P)$ is β -stable if $\beta([y]) = y$ for all $y \in W$. For example, the set $\{\beta(\emptyset), \beta(\{\beta(\emptyset)\}), \beta(\{\beta(\emptyset), \beta(\{\beta(\emptyset)\})\})\}$ is β -stable, and it certainly can be enlarged by any amount to the right. For any two β -stable sets $U, W \in \mathcal{W}(P)$ with common minimal element, either $U \subset W$ or $W \subset U$

¹¹Such an element is unique, as we have seen above.

holds, because the minimal elements $u \in U \setminus (U \cap W)$ and $w \in W \setminus (U \cap W)$ are each the β -image of the same initial segment $[u] = [w] \subset U \cap W$ and therefore must be equal.

Exercise 1.18 Check that the union of all β -stable sets having the same minimal element $p \in P$ is well ordered and β -stable.

Let U be some union from [Exercise 1.18](#). Then $\beta(U)$ cannot be an exterior upper bound for U , because otherwise, $U \cup \{\beta(U)\}$ would be a β -stable set with the same minimal point as U , which forces it to be a subset of U . Contradiction. \square

Corollary 1.1 (Zorn's Lemma I) *Suppose that every well-ordered subset in a poset P has an upper bound, not necessarily exterior. Then there exists a maximal element in P .*

Proof Assume the contrary. Then for all $x \in P$ there exists $y > x$. Hence, the axiom of choice allows us to choose some *exterior* upper bound¹² $b(W)$ for every $W \in \mathcal{W}(P)$. The resulting map $W \mapsto b(W)$ contradicts [Lemma 1.2](#). \square

Exercise 1.19 (Bourbaki–Witt Fixed-Point Lemma) Under the assumption of [Corollary 1.1](#), show that every map $f : P \rightarrow P$ such that $f(x) \geq x$ for all $x \in X$ has a fixed point, i.e., that there exists $p \in P$ such that $f(p) = p$.

Definition 1.2 (Complete Posets) A partially ordered set is said to be *complete* if every totally ordered (with respect to the order on P) subset in P has an upper bound, not necessarily exterior.

Lemma 1.3 (Zorn's Lemma II) *Every complete poset P has a maximal element.*

Proof Every complete poset surely satisfies the assumption of [Corollary 1.1](#). \square

Problems for Independent Solution to Chap. 1

Problem 1.1 Find the total number of maps from a set of cardinality 6 to a set of cardinality 2 such that every point of the target set has at least two elements in its preimage.

Problem 1.2 Let X, Y be finite sets, $|X| \geq |Y|$. How many right inverse maps does a given surjection $X \twoheadrightarrow Y$ have? How many left inverse maps does a given injection $Y \hookrightarrow X$ have?

¹²To be more precise (see [Sect. 1.3.2](#) on p. 11), let $I \subset \mathcal{W} \times P$ consist of all pairs (W, c) such that $w < c$ for all $w \in W$. Then the projection $\pi_1 : I \rightarrow \mathcal{W}$, $(W, c) \mapsto W$, is surjective, because by the assumption of the lemma, for every W , there exists some upper bound d , and then we have assumed that there exists some $c > d$. Take $b : \mathcal{W} \rightarrow P$ to be the composition $\pi_2 \circ g$, where $g : \mathcal{W} \rightarrow I$ is any section of π_1 followed by the projection $\pi_2 : I \rightarrow P$, $(W, c) \mapsto c$.

Problem 1.3 How many distinct “words” (i.e., strings of letters, not necessarily actual words) can one get by permuting the letters in the words:

$$\begin{aligned} & \text{(a) algebra, (b) syzygy, (c) } \underbrace{aa \dots a}_{\alpha} \underbrace{bb \dots b}_{\beta}, \\ & \text{(d) } \underbrace{a_1 a_1 \dots a_1}_{\alpha_1} \underbrace{a_2 a_2 \dots a_2}_{\alpha_2} \dots \underbrace{a_m a_m \dots a_m}_{\alpha_m} ? \end{aligned}$$

Problem 1.4 Expand and collect like terms in (a) $(a_1 + a_2 + \dots + a_m)^2$, (b) $(a + b + c)^3$.

Problem 1.5 Given $m, n \in \mathbb{N}$, how many solutions does the equation $x_1 + x_2 + \dots + x_m = n$ have in (a) positive, (b) nonnegative, integers x_1, x_2, \dots, x_m ?

Problem 1.6 Count the number of monomials in n variables that have total degree¹³ (a) exactly d , (b) at most d .

Problem 1.7 Is $1000! / (100!)^{10}$ an integer?

Problem 1.8 For a prime $p \in \mathbb{N}$, show that every binomial coefficient $\binom{p}{k}$ with $1 \leq k \leq (p-1)$ is divisible by p .

Problem 1.9 Evaluate the sums: (a) $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n}$, (b) $\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \dots$, (c) $\binom{k}{k} + \binom{k+1}{k} + \dots + \binom{k+n}{k}$, (d) $\binom{n}{1} + 2\binom{n}{2} + \dots + n\binom{n}{n}$, (e) $\binom{n}{0} + 2\binom{n}{1} + \dots + (n+1)\binom{n}{n}$, (f) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \dots + (-1)^n \binom{n}{n}$, (g) $\binom{n}{0}^2 + \binom{n}{1}^2 + \dots + \binom{n}{n}^2$.

Problem 1.10 For given $m, n \in \mathbb{N}$, count the total number of (a) arbitrary, (b) bijective, (c) strictly increasing, (d) injective, (e) nonstrictly increasing, (f) nonstrictly increasing and surjective, (g) surjective maps $\{1, 2, \dots, m\} \rightarrow \{1, 2, \dots, n\}$.

Problem 1.11 Count the total number of Young diagrams (a) of weight 6, (b) of weight 7 and length at most 3, (c) having at most p rows and q columns.

Problem 1.12* (by L. G. Makar-Limanov). A soda jerk is whiling away the time manipulating 15 disposable cups stacked on a table in several vertical piles. During each manipulation, he removes the topmost cup of each pile and stacks these together to form a new pile. What can you say about the distribution of cups after 1000 such manipulations?

Problem 1.13 Given four distinct cups, four identical glasses, ten identical sugar cubes, and seven cocktail straws each in different color of the rainbow, count the number of distinct arrangements of (a) straws between cups, (b) sugar between cups, (c) sugar between glasses, (d) straws between glasses. (e) Answer the same questions under the constraint that every cup or glass must have at least one straw or sugar cube (possibly one or more of each) in it.

Problem 1.14 The sides of a regular planar n -gon lying in three-dimensional space are painted in n fixed different colors, one color per side, in all possible ways. How many different painted n -gons do we get if two colored n -gons are considered the same if one can be obtained from the other by some motion in three-space?

¹³The total degree of the monomial $x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}$ equals $\sum_{i=1}^n m_i$.

Problem 1.15 How many different necklaces can be made from 5 red, 7 blue, and 11 white otherwise identical glass beads?

Problem 1.16 All the faces of a regular (a) cube, (b) tetrahedron, are painted using six fixed colors (different faces in distinct colors) in all possible ways. How many different painted polyhedra do we get?

Problem 1.17 How many different knick-knacks do we get by gluing pairs of the previously painted (a) cubes, (b) tetrahedra face to face randomly?

Problem 1.18 Show that Zorn's lemma, Lemma 1.3, is equivalent to the axiom of choice. More precisely, assume that Lemma 1.3 holds for every poset P and prove that every surjective map $f : X \twoheadrightarrow Y$ admits a section. Hint: consider the set of maps $g_U : U \rightarrow X$ such that $U \subset Y$ and $fg_U = \text{Id}_U$; equip it with a partial order, where $g_U \leq g_W$ means that $U \subset W$ and $g_W|_U = g_U$; verify that Lemma 1.3 can be applied; prove that every maximal g_U has $U = Y$.

Problem 1.19 (Hausdorff's Maximal Chain Theorem) Use Lemma 1.3, Zorn's lemma, to prove that every chain in every poset is contained in some maximal (with respect to inclusion) chain. Hint: consider the set of all chains containing a given chain; equip it with the partial order provided by inclusion; then proceed as in the previous problem.

Problem 1.20 (Zermelo's Theorem) Write $\mathcal{S}(X)$ for the set of all nonempty subsets in a given set X including X itself. Use the axiom of choice to construct a map $\mu : \mathcal{S}(X) \rightarrow X$ such that $\mu(Z) \in Z$ for all $Z \in \mathcal{S}(X)$. Write $\mathcal{W}(X)$ for the set of all $W \in \mathcal{S}(X)$ possessing a well ordering such that $\mu(W \setminus [w]) = w$ for all $w \in W$. Verify that $\mathcal{W}(X) \neq \emptyset$, and modify the proof of Lemma 1.2 on p. 15 to show that $X \in \mathcal{W}(X)$. This means that *every set can be well ordered*.

Chapter 2

Integers and Residues

2.1 Fields, Rings, and Abelian Groups

2.1.1 Definition of a Field

Given a set X , a map $X \times X \rightarrow X$ is called a *binary operation* on X . Addition and multiplication of rational numbers are binary operations on the set \mathbb{Q} taking $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ to $a + b \in \mathbb{Q}$ and $ab \in \mathbb{Q}$ respectively. Informally speaking, a *field* is a numeric domain whose elements can be added, subtracted, multiplied, and divided by the same rules that apply to rational numbers. The precise definition given below takes these rules as axioms.

Definition 2.1 A set \mathbb{F} equipped with two binary operations $\mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$, *addition* $(a, b) \mapsto a + b$ and *multiplication* $(a, b) \mapsto ab$, is called a *field* if these operations satisfy the following three collections of axioms:

PROPERTIES OF ADDITION

$$\text{commutativity: } a + b = b + a \quad \forall a, b \in \mathbb{F} \quad (2.1)$$

$$\text{associativity: } a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{F} \quad (2.2)$$

$$\text{existence of zero: } \exists 0 \in \mathbb{F} : a + 0 = a \quad \forall a \in \mathbb{F} \quad (2.3)$$

$$\text{existence of opposites: } \forall a \in \mathbb{F} \quad \exists (-a) \in \mathbb{F} : a + (-a) = 0 \quad (2.4)$$

PROPERTIES OF MULTIPLICATION

$$\text{commutativity: } ab = ba \quad \forall a, b \in \mathbb{F} \quad (2.5)$$

$$\text{associativity: } a(bc) = (ab)c \quad \forall a, b, c \in \mathbb{F} \quad (2.6)$$

$$\text{existence of unit: } \exists 1 \in \mathbb{F} : 1a = a \quad \forall a \in \mathbb{F} \quad (2.7)$$

$$\text{existence of inverses: } \forall a \in \mathbb{F} \setminus 0 \quad \exists a^{-1} \in \mathbb{F} : aa^{-1} = 1 \quad (2.8)$$

RELATIONS BETWEEN ADDITION AND MULTIPLICATION

$$\text{distributivity:} \quad a(b + c) = ab + ac \quad \forall a, b, c \in \mathbb{F} \quad (2.9)$$

$$\text{nontriviality:} \quad 0 \neq 1 \quad (2.10)$$

Example 2.1 (Field of Two Elements) The simplest set that satisfies Definition 2.1 consists of the two elements 0, 1, with $0 + 1 = 1 \cdot 1 = 1$ and all the other sums and products equal to 0 (including $1 + 1 = 0$). It is denoted by \mathbb{F}_2 .

Exercise 2.1 Verify that \mathbb{F}_2 satisfies all the axioms of Definition 2.1.

Elements of \mathbb{F}_2 can be interpreted either as residue classes modulo 2 added and multiplied by the rules (1.17) from Example 1.4 on p. 8 or as logical “false” = 0 and “true” = 1. In the latter case, addition and multiplication become logical “XOR” and “AND” respectively,¹ and algebraic expressions in \mathbb{F}_2 can be thought of as logical predicates.

Exercise 2.2 Write down a polynomial in x with coefficients in \mathbb{F}_2 that evaluates to NOT x and a polynomial in x, y that evaluates to x OR y .²

Example 2.2 (Rational Numbers) The field of rational numbers \mathbb{Q} is the main motivating example for Definition 2.1. As a set, \mathbb{Q} consists of fractions a/b , which are equivalence classes³ of pairs (a, b) , where $a, b \in \mathbb{Z}$, $b \neq 0$, modulo the equivalence generated by the relations

$$(a, b) \sim (sa, sb) \quad \forall s \in \mathbb{Z} \setminus 0. \quad (2.11)$$

This equivalence is exhausted by the relations

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{for all} \quad a_1 b_2 = a_2 b_1, \quad (2.12)$$

and each relation (2.12) can be achieved by at most a two-step chain of relations (2.11). Addition and multiplication of fractions are defined by the rules

$$\frac{a}{b} + \frac{c}{d} \stackrel{\text{def}}{=} \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} \stackrel{\text{def}}{=} \frac{ac}{bd}. \quad (2.13)$$

¹Logical “exclusive OR” (XOR): $a + b$ is true if and only if precisely one of a, b is true (and not both). Logical AND: $a \cdot b$ is true if and only if both a and b are true.

²Logical NOT x evaluates to true if and only if x is false. Nonexclusive x OR y is true if and only if at least one of x and y is true.

³See Example 1.5 on p. 9.

Exercise 2.3 Verify the consistency of these definitions⁴ and that axioms (2.1)–(2.10) are satisfied.

Example 2.3 (Real Numbers) The set of real numbers \mathbb{R} can be defined in several ways: either as a set of equivalence classes of rational Cauchy sequences,⁵ or as the set of Dedekind sections⁶ of \mathbb{Q} , or as the set of equivalence classes of infinite decimal⁷ fractions.⁸ Whichever definition of \mathbb{R} is chosen, the description of addition and multiplication as well as verification of axioms (2.1)–(2.10) requires some intellectual effort, which is generally undertaken in the first chapters of a course in real analysis. I hope that you have taken such a course.

2.1.2 Commutative Rings

A set K equipped with addition and multiplication is called a *commutative ring with unit* if these operations satisfy all the axioms of Definition 2.1 on p. 19 except for (2.8). This means that not all nonzero elements are invertible. The main motivating examples of commutative rings with unit are provided by the ring of integers \mathbb{Z} and the rings $K[x]$ of polynomials in the variable x with coefficients in an arbitrary commutative ring K with unit.

If the existence of a unit and the nontriviality axioms (2.7), (2.10) are also excluded along with (2.8) from Definition 2.1 on p. 19, a set K equipped with two operations possessing all the remaining properties is called just a *commutative ring*. The even integers and the polynomials with even integer coefficients are examples of commutative rings without a unit. The *zero ring*, consisting of only the zero element, is also a commutative ring.

2.1.3 Abelian Groups

A set A equipped with one binary operation $A \times A \rightarrow A$ is called an *abelian group* if the operation satisfies the first four axioms (2.1)–(2.4) from Definition 2.1, i.e., if it is commutative and associative, and possesses a zero element as well as opposite

⁴That is, check that the equivalence classes of the results are not changed when the operands are replaced by equivalent fractions.

⁵A sequence is said to be *Cauchy* if for every positive ε , all but a finite number of elements of the sequence lie within an interval of length ε . Two Cauchy sequences $\{a_n\}$, $\{b_n\}$ are equivalent if the sequence $\{a_1, b_1, a_2, b_2, \dots\}$ is Cauchy.

⁶A Dedekind section is a partition $\mathbb{Q} = X \sqcup Y$ such that there is no minimal element in Y and $x < y$ for all $x \in X$, $y \in Y$.

⁷Or any other positional scale of notation.

⁸Such an equivalence identifies the decimal $a_1a_2 \dots a_n.b_1b_2 \dots b_m999\dots$ with the decimal $a_1a_2 \dots a_n.b_1b_2 \dots b_{m-1}(b_m + 1)000\dots$, where a_i, b_j are decimal digits and $b_m \neq 9$.

elements to all $a \in A$. Thus, every commutative ring K is an abelian group with respect to addition. This group is called the *additive group* of the ring K . The main motivating example of an abelian group not related directly to a ring is provided by *vectors*.

Example 2.4 (Geometric Vectors) In the framework of Euclidean geometry as studied in high school, let us declare two directed segments to be equivalent if they are parallel displacements of each other. The equivalence classes of directed segments are called *geometric vectors*. The *zero vector*, i.e., the class of the empty segment, is also considered a vector. Vectors can be depicted by arrows considered up to a translation in the plane. An *addition of vectors* is defined by the *triangle rule*: translate the arrows representing vectors a, b in such a way that the head of a coincides with the tail of b and declare $a + b$ to be an arrow going from the tail of a to the head of b . Commutativity and associativity of addition are established by means of the *parallelogram* and *quadrangle* diagrams shown in Figs. 2.1 and 2.2:

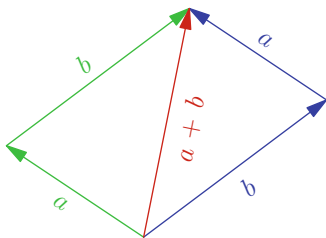


Fig. 2.1 The parallelogram rule

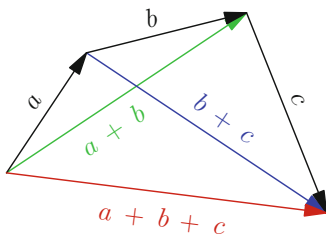


Fig. 2.2 The quadrangle rule

The opposite vector $-a$ of a is obtained by reversing the direction of a .

Example 2.5 (The Multiplicative Group of a Field) The properties of multiplication listed in axioms (2.5)–(2.8) from Definition 2.1 on p. 19 assert that the set of nonzero elements in a field \mathbb{F} is an abelian group with respect to multiplication. This group is called the *multiplicative group* of \mathbb{F} and is denoted by $\mathbb{F}^* \stackrel{\text{def}}{=} \mathbb{F} \setminus 0$. The role of the

zero element in the multiplicative group is played by the unit. In an abstract abelian group, such an element is called the *identity element* or *neutral element* of the group. The multiplicative version of the opposite is provided by the inverse element.

Lemma 2.1 *In every abelian group A , the neutral element is unique, and for each $a \in A$, its opposite $-a$ is uniquely determined by a . In particular, $-(-a) = a$.*

Proof Let us write $+$ for the operation in A . If there are two identity elements 0_1 and 0_2 , then $0_1 = 0_1 + 0_2 = 0_2$, where the first equality holds because 0_2 is an identity element, and the second holds because 0_1 is an identity element. If there are two elements $-a$ and $-a'$ both opposite to a , then $-a = (-a) + 0 = (-a) + (a + (-a')) = ((-a) + a) + (-a') = 0 + (-a') = -a'$. \square

Lemma 2.2 *In every commutative ring K , the equality $0 \cdot a = 0$ holds for all $a \in K$. If K has a unit, then for every $a \in A$, the product $(-1) \cdot a$ equals the opposite element of a .*

Proof Let $a \cdot 0 = b$. Then $b + a = a \cdot 0 + a = a \cdot 0 + a \cdot 1 = a(0 + 1) = a \cdot 1 = a$. Adding $(-a)$ to both sides, we get $b = 0$. The second statement follows from the computation $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = ((-1) + 1) \cdot a = 0 \cdot a = 0$. \square

Remark 2.1 In the presence of all the other axioms, the nontriviality axiom (2.10) in the definition of a field is equivalent to the requirement $\mathbb{F} \neq \{0\}$. Indeed, if $0 = 1$, then for each $a \in \mathbb{F}$, we get $a = a \cdot 1 = a \cdot 0 = 0$.

2.1.4 Subtraction and Division

It follows from Lemma 2.1 that in every abelian group, a *subtraction operation* is well defined by the rule

$$a - b \stackrel{\text{def}}{=} a + (-b). \quad (2.14)$$

In particular, subtraction is defined in the additive group of every commutative ring.

It follows from Lemma 2.1 and Lemma 2.2 applied to the multiplicative group of a field that every field \mathbb{F} has a unique unit and for every $a \in \mathbb{F}^*$, its inverse element a^{-1} is uniquely determined by a . Therefore, \mathbb{F}^* admits a *division operation* defined by the rule

$$a/b \stackrel{\text{def}}{=} ab^{-1}, \text{ where } b \neq 0. \quad (2.15)$$

2.2 The Ring of Integers

2.2.1 Divisibility

An element a in a commutative ring K with unit is said to be *invertible* if there exists an element $a^{-1} \in K$ such that $a^{-1}a = 1$. Otherwise, a is *noninvertible*. In the ring of integers \mathbb{Z} , there are just two invertible elements: ± 1 . In the ring $\mathbb{Q}[x]$ of polynomials in x with rational coefficients, the invertible elements are the nonzero constants, i.e., the nonzero polynomials of degree zero.

An element a in a commutative ring K is said to be *divisible* by $b \in K$ if there is an element $q \in K$ such that $a = bq$. In this case, we write $b \mid a$ or $a:b$ and call q the *quotient* of a by b . Divisibility is closely related to the solvability of linear equations.

2.2.2 The Equation $ax + by = k$ and the Greatest Common Divisor in \mathbb{Z}

Let us fix some $a, b \in \mathbb{Z}$ and write

$$(a, b) \stackrel{\text{def}}{=} \{ax + by \mid x, y \in \mathbb{Z}\} \quad (2.16)$$

for the set of all integers represented as $ax + by$ for some integers x, y . This set is a subring of \mathbb{Z} , and for every $z \in (a, b)$, all its multiples mz lie in (a, b) as well. Note that we have $a, b \in (a, b)$, and every element of (a, b) is divisible by every common divisor of a and b . Write d for the smallest positive number in (a, b) . For every $z \in (a, b)$, the remainder r of division of z by d lies in (a, b) , because $r = z - kd$ and both of z, kd lie in the ring (a, b) . Since $0 \leq r < d$, we conclude that $r = 0$ by the choice of d . Thus, the set (a, b) coincides with the set of all multiples of d . Therefore, d divides both a and b and is divisible by every common divisor of a and b . The number d is called the *greatest common divisor* of $a, b \in \mathbb{Z}$ and is denoted by $\text{GCD}(a, b)$.

By the way, the arguments above demonstrate that for given $a, b, n \in \mathbb{Z}$, the equation $ax + by = n$ is solvable in $x, y \in \mathbb{Z}$ if and only if $n \mid \text{GCD}(a, b)$.

Exercise 2.4 Given an arbitrary finite collection of numbers $a_1, a_2, \dots, a_m \in \mathbb{Z}$, use an appropriate generalization of the previous construction to produce a number $d = a_1x_1 + a_2x_2 + \dots + a_mx_m$, $x_i \in \mathbb{Z}$, that divides all the a_i and is divisible by all common divisors of the a_i . Prove that the equation $a_1x_1 + a_2x_2 + \dots + a_mx_m = n$ is solvable in $x_i \in \mathbb{Z}$ if and only if $n \mid d$.

The number d from [Exercise 2.4](#) is denoted by $\text{GCD}(a_1, a_2, \dots, a_m)$ and called the *greatest common divisor* of a_1, a_2, \dots, a_m .

2.2.3 The Euclidean Algorithm

The Euclidean algorithm computes $\text{GCD}(a, b)$ together with the expansion $\text{GCD}(a, b) = ax + by$ as follows. Let $a \geq b$. Put

$$E_0 = a, E_1 = b, E_k = \text{remainder of division of } E_{k-2} \text{ by } E_{k-1} \text{ (for } k \geq 1). \quad (2.17)$$

The numbers E_k are strictly decreasing until some E_r divides E_{r-1} , and we get $E_{r+1} = 0$. The last nonzero number E_r in the sequence E_k is equal to $\text{GCD}(a, b)$.

Exercise 2.5 Prove this.

During the calculations, it is not onerous to write down all the numbers E_k in the form $x \cdot E_0 + y \cdot E_1$. This leads to the required representation $E_r = x \cdot E_0 + y \cdot E_1$. For example, for $a = 10\,203$ and $b = 4687$, the computation consists of seven steps:

$$\begin{aligned} E_0 &= 10\,203 \\ E_1 &= 4\,687 \\ E_2 &= 829 = E_0 - 2E_1 = +1E_0 - 2E_1 \\ E_3 &= 542 = E_1 - 5E_2 = -5E_0 + 11E_1 \\ E_4 &= 287 = E_2 - E_3 = +6E_0 - 13E_1 \\ E_5 &= 255 = E_3 - E_4 = -11E_0 + 24E_1 \\ E_6 &= 32 = E_4 - E_5 = +17E_0 - 37E_1 \\ E_7 &= 31 = E_5 - 7E_6 = -130E_0 + 283E_1 \\ E_8 &= 1 = E_6 - E_7 = +147E_0 - 320E_1 \\ [E_9 &= 0 = E_7 - 31E_8 = -4687E_0 + 10\,203E_1]. \end{aligned} \quad (2.18)$$

This shows that $\text{GCD}(10\,203, 4687) = 1 = 147 \cdot 10\,203 - 320 \cdot 4687$. The bottom row in brackets was included to check the result. Moreover, it computes the *least common multiple* $\text{LCM}(a, b)$ together with the associated factors $\text{LCM}(a, b)/a$ and $\text{LCM}(a, b)/b$.

Exercise 2.6 Prove that in the expression $0 = E_{r+1} = q_0E_0 + q_1E_1$, which appears after the last step of the Euclidean algorithm, the absolute value $|q_0E_0| = |q_1E_1|$ is equal to $\text{LCM}(a, b)$.

Remark 2.2 The Euclidean algorithm is much, much faster than prime factorization. To convince yourself of this, just try calculate the prime factorizations for 10 203 or 4687 by hand and compare this with the hand calculation (2.18). Given the product

of two *very* large prime numbers, recovering those primes is too difficult even for supercomputers. Many data encryption systems are based on this fact.

2.3 Coprime Elements

In the ring \mathbb{Z} , the condition $\text{GCD}(a, b) = 1$ is equivalent to the solvability of the equation $ax + by = 1$ in x, y . Integers a, b for which this equation is solvable are said to be *coprime*.

For an arbitrary commutative ring K with unit, the solvability of the equation $ax + by = 1$ forces every common divisor of a, b to be invertible in K , because $a = d\alpha, b = d\beta$, and $ax + by = 1$ imply $d(\alpha + \beta) = 1$. However, if all common divisors of a, b are invertible, the equation $ax + by = 1$ may be unsolvable in general. For example, in the ring $\mathbb{Q}[x, y]$ of polynomials in x, y with rational coefficients, the monomials x and y do not have nonconstant common divisors, but the equality $f(x, y) \cdot x + g(x, y) \cdot y = 1$ fails for all $f, g \in \mathbb{Q}[x, y]$.

Exercise 2.7 Explain why.

Nevertheless, just the solvability of $ax + by = 1$ leads to most of the nice properties of a, b known for coprime integers. Therefore, for arbitrary rings the next definition is reasonable.

Definition 2.2 Elements a, b of an arbitrary commutative ring K with unit are called *coprime* if the equation $ax + by = 1$ is solvable in $x, y \in K$.

Lemma 2.3 Let K be an arbitrary commutative ring with unit and let $a, b \in K$ be coprime. Then for every $c \in K$,

$$b \mid ac \Rightarrow b \mid c, \quad (2.19)$$

$$a \mid c \text{ \& } b \mid c \Rightarrow ab \mid c. \quad (2.20)$$

Furthermore, if $a \in K$ is coprime to each of b_1, b_2, \dots, b_n , then a is coprime to their product $b_1 \cdot b_2 \cdots b_n$.

Proof Multiplying both sides of $ax + by = 1$ by c , we get the equality $c = acx + bcy$, which gives both implications (2.19), (2.20). If for each $i = 1, 2, \dots, n$, there exist $x_i, y_i \in K$ such that $ax_i + b_i y_i = 1$, then by multiplying all these equalities together and expanding on the left-hand side, we get

$$(b_1 b_2 \cdots b_n) \cdot (y_1 y_2 \cdots y_n) + \text{monomials divisible by } a = 1.$$

This leads to the required equality $a \cdot (\text{something}) + (b_1 b_2 \cdots b_n) \cdot (y_1 y_2 \cdots y_n) = 1$.

□

Exercise 2.8 Use Lemma 2.3 to prove the *factorization theorem* for \mathbb{Z} : each element $n \in \mathbb{Z}$ is equal to a finite product of prime integers⁹ and any two prime factorizations

$$p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_m$$

have $k = m$ and (after appropriate renumbering of the factors) $p_i = \pm q_i$ for all i .

Remark 2.3 (GCD in an Arbitrary Commutative Ring) Given two elements a, b in a commutative ring K , an element $d \in K$ dividing both a and b and divisible by every common divisor of a and b is called a *greatest common divisor* of a and b . A greatest common divisor may not exist in general. If it exists, it may not be unique, and it may not be representable as $d = ax + by$. If a ring K possesses a unit, then for every greatest common divisor d of a and b and invertible element $s \in K$, the product sd is a greatest common divisor of a and b as well.

2.4 Rings of Residues

2.4.1 Residue Classes Modulo n

Recall¹⁰ that two numbers $a, b \in \mathbb{Z}$ are said to be *congruent modulo n* if n divides $a - b$, and in this case, we write $a \equiv b \pmod{n}$. We know from Example 1.4 on p. 8 that congruence modulo n is an equivalence relation that decomposes \mathbb{Z} into a disjoint union of equivalence classes called *residue classes modulo n* . We write $\mathbb{Z}/(n)$ for the set of residue classes and denote the residue class of an integer $a \in \mathbb{Z}$ by $[a]_n \in \mathbb{Z}/(n)$. Note that the same residue class may be written in many different ways: $[x]_n = [y]_n$ if and only if $x = y + dn$ for some $d \in \mathbb{Z}$. Nevertheless, by Exercise 1.10 on p. 9, the addition and multiplication of residue classes are well defined by the rules

$$[a] + [b] \stackrel{\text{def}}{=} [a + b], \quad [a] \cdot [b] \stackrel{\text{def}}{=} [ab], \quad (2.21)$$

in the sense that the resulting residue classes do not depend on the choice of $a, b \in \mathbb{Z}$ representing the classes $[a], [b] \in \mathbb{Z}/(n)$. The operations (2.21) clearly satisfy the definition of a commutative ring with unit, because their right-hand sides deal with the operations within the commutative ring \mathbb{Z} , where all the axioms hold. Thus, $\mathbb{Z}/(n)$ is a commutative ring with unit. It consists of n elements, which can be written, e.g., as $[0]_n, [1]_n, \dots, [(n-1)]_n$.

⁹An integer is *prime* if it is not equal to the product of two noninvertible integers.

¹⁰See Sect. 1.2 on p. 7.

2.4.2 Zero Divisors and Nilpotents

In $\mathbb{Z}/(10)$, the product of nonzero classes $[2] \cdot [5] = [10]$ equals zero. Similarly, in $\mathbb{Z}/(8)$, the nonzero element $[2]$ has a zero cube: $[2]^3 = [8] = [0]$.

In an arbitrary commutative ring K , a nonzero element $a \in K$ is called a *zero divisor* if $ab = 0$ for some nonzero $b \in K$. Note that an invertible element $a \in K$ cannot divide zero, because multiplication of both sides of the equality $ab = 0$ by a^{-1} forces $b = 0$. In particular, a commutative ring with zero divisors cannot be a field.

A commutative ring K with unit is called an *integral domain* if there are no zero divisors in K . For example, \mathbb{Z} and $\mathbb{Q}[x]$ are both integral domains.

A nonzero element $a \in K$ is called *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$. Clearly, every nilpotent element is a zero divisor. A commutative ring K with unit is called *reduced* if there are no nilpotent elements in K . Therefore, every integral domain is reduced.

Exercise 2.9 Prove that if a is a nilpotent element in a commutative ring with unit, then $1 + a$ is invertible.

2.4.3 Invertible Elements in Residue Rings

A residue class $[m]_n \in \mathbb{Z}/(n)$ is invertible if and only if $[m]_n[x]_n = [mx]_n = [1]_n$ for some $[x]_n \in \mathbb{Z}/(n)$. The latter means the existence of $x, y \in \mathbb{Z}$ such that $mx + ny = 1$ in \mathbb{Z} . Such x, y exist if and only if $\text{GCD}(m, n) = 1$ in \mathbb{Z} . This can be checked by the Euclidean algorithm, which allows us to find the required (x, y) as well if m, n are coprime. Thus, the residue class $[x]$ inverse to $[m]$, if it exists, can be easily computed. For example, the calculations made in formula (2.18) on p. 25 show that the class $[10\ 203]$ is invertible in $\mathbb{Z}/(4687)$ and $[10\ 203]_{4687}^{-1} = [147]_{4687}$. At the same time, we conclude that the class $[4687]$ is invertible in $\mathbb{Z}/(10\ 203)$ and $[4687]^{-1} = -[320]$ in $\mathbb{Z}/(10\ 203)$.

The invertible elements of a commutative ring K with unit form a multiplicative abelian group called the *group of invertible elements*¹¹ and denoted by K^* .

The group $\mathbb{Z}/(n)^*$ of *invertible residue classes* consists of classes $[m]_n \in \mathbb{Z}/(n)$ such that $\text{GCD}(m, n) = 1$. The order¹² of this group is equal to the number of positive

¹¹In other terminology, the *group of units*.

¹²The order of a group is the number of its elements.

integers m that are strictly less than n and coprime to n . This number is denoted by

$$\varphi(n) \stackrel{\text{def}}{=} |\mathbb{Z}/(n)^*|.$$

The map $\varphi : \mathbb{N} \rightarrow \mathbb{N}$, $n \mapsto \varphi(n)$, is called *Euler's φ -function*.

2.4.4 Residue Fields

It follows from the above description of invertible residue classes that the ring $\mathbb{Z}/(n)$ is a field if and only if n is a prime number, because only a prime number p is coprime to all positive integers less than p . For a prime $p \in \mathbb{N}$, the residue class field $\mathbb{Z}/(p)$ is denoted by \mathbb{F}_p .

Example 2.6 (Binomial Formula Modulo p) For a prime $p \in \mathbb{N}$, there is a remarkable identity in the residue class field $\mathbb{F}_p = \mathbb{Z}/(p)$, namely

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} = 0. \quad (2.22)$$

It forces the sum of m ones to vanish as soon m is a multiple of p . In particular, the sum of

$$\binom{p}{k} = \frac{p(p-1) \cdots (p-k+1)}{k(k-1) \cdots 1}$$

ones vanishes for all $1 \leq k \leq (p-1)$. Indeed, by Lemma 2.3 on p. 26, for such k , the number p is coprime to the product in the denominator. Then by the same lemma, the denominator divides the product $(p-1) \cdots (p-k+1)$. Therefore, the entire quotient is divisible by p .

We conclude that in \mathbb{F}_p , the binomial formula (1.7) on p. 6 becomes

$$(a + b)^p = a^p + b^p, \quad (2.23)$$

because after expanding the left-hand side as explained in Example 2.3 on p. 5, we get for each k exactly $\binom{p}{k}$ similar monomials $a^k b^{p-k}$, producing the sum of $\binom{p}{k}$ ones as the coefficient of $a^k b^{p-k}$ on the right-hand side.

Exercise 2.10 Prove the congruence

$$\binom{mp^n}{p^n} \equiv m \pmod{p}$$

for every prime $p \in \mathbb{N}$ and all $m \in \mathbb{N}$ coprime to p .

Theorem 2.1 (Fermat's Little Theorem) $a^p \equiv a \pmod{p}$ for every $a \in \mathbb{Z}$ and prime $p \in \mathbb{N}$.

Proof We have to show that $[a^p] = [a]$ in \mathbb{F}_p . This follows immediately from (2.23):

$$\begin{aligned} [a]^p &= \underbrace{([1] + [1] + \cdots + [1])^p}_{a \text{ times}} = \underbrace{[1]^p + [1]^p + \cdots + [1]^p}_{a \text{ times}} \\ &= \underbrace{[1] + [1] + \cdots + [1]}_{a \text{ times}} = [a]. \end{aligned}$$

□

2.5 Direct Products of Commutative Groups and Rings

The set-theoretic product

$$\prod_v A_v = A_1 \times A_2 \times \cdots \times A_m = \{(a_1, a_2, \dots, a_m) \mid a_v \in A_v\} \quad (2.24)$$

of abelian groups A_1, A_2, \dots, A_m possesses the structure of an abelian group with addition defined by

$$(a_1, a_2, \dots, a_m) + (b_1, b_2, \dots, b_m) \stackrel{\text{def}}{=} (a_1 + b_1, a_2 + b_2, \dots, a_m + b_m), \quad (2.25)$$

where the i th components are added within the i th group A_i .

Exercise 2.11 Verify that addition (2.25) is commutative and associative, its neutral element is $(0, 0, \dots, 0)$, and the opposite element to (a_1, a_2, \dots, a_m) is the element $(-a_1, -a_2, \dots, -a_m)$.

The abelian group $\prod A_v$ obtained in this way is called the *direct product* of abelian groups A_i . If all the groups A_i are finite, their direct product is also finite, of order $|\prod A_i| = \prod |A_i|$. The direct product is well defined for any family of abelian groups A_x indexed by elements $x \in X$ of an arbitrary set X , not necessarily finite. We write $\prod_{x \in X} A_x$ for such a product.

Similarly, a direct product of commutative rings K_x , where x runs through some set X , consists of families $(a_x)_{x \in X}$ formed by elements $a_x \in K_x$. Addition and multiplication of such families is defined componentwise:

$$(a_x)_{x \in X} + (b_x)_{x \in X} = (a_x + b_x)_{x \in X}, \quad (a_x)_{x \in X} \cdot (b_x)_{x \in X} = (a_x \cdot b_x)_{x \in X}.$$

The resulting ring is denoted by $\prod_{x \in X} K_x$ as well.

Exercise 2.12 Check that $\prod K_x$ actually is a commutative ring. If each K_x has unit $1_x \in K_x$, verify that the family $(1_x)_{x \in X}$ is the unit in $\prod K_x$.

For example, let $X = \mathbb{R}$ and all $K_x = \mathbb{R}$ as well. Then the product $\prod_{x \in \mathbb{R}} \mathbb{R}_x$ formed by \mathbb{R} copies of \mathbb{R} is isomorphic to the ring of all functions $f : \mathbb{R} \rightarrow \mathbb{R}$, where the operations are the usual addition and multiplication of functions. The isomorphism takes a family of real numbers $(f_x) \in \prod_{x \in \mathbb{R}} \mathbb{R}_x$ to the function $f : \mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto f_x$.

If some element $a_x \in K_x$ in the family $(a_x) \in \prod K_x$, with not all the a_x equal to zero, either equals zero or divides zero in K_x , then the family is a zero divisor in $\prod K_x$. For example, $(0, 1, \dots, 1)$ divides zero, because of

$$(0, 1, \dots, 1) \cdot (1, 0, \dots, 0) = (0, 0, \dots, 0).$$

Thus, the direct product of more than one ring cannot be a field.

Exercise 2.13 Show that for two given prime numbers $p, q \in \mathbb{N}$, the product $\mathbb{F}_p \times \mathbb{F}_q$ consists of the zero element, $(p-1)(q-1)$ invertible elements, and $p+q-2$ zero divisors $(a, 0)$, $(0, b)$, where $a \neq 0$ and $b \neq 0$. Note that $(\mathbb{F}_p \times \mathbb{F}_q)^* \simeq \mathbb{F}_p^* \times \mathbb{F}_q^*$.

If all rings K_x possess units, then the invertible elements in the direct product $\prod K_x$ are exactly those sequences (a_x) such that each a_x is invertible in K_x . Therefore, the group of invertible elements in $\prod K_x$ coincides with the direct product of groups K_x^* :

$$\left(\prod K_x\right)^* = \prod K_x^* \quad (2.26)$$

2.6 Homomorphisms

2.6.1 Homomorphisms of Abelian Groups

A map of abelian groups $\varphi : A \rightarrow B$ is called a *homomorphism* if it respects the group operation, that is, if for all $a_1, a_2 \in A$, the equality

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) \quad (2.27)$$

holds in the group B .

Exercise 2.14 Verify that the composition of homomorphisms is again a homomorphism.

Lemma 2.4 For every homomorphism of abelian groups $\varphi : A \rightarrow B$, the equalities

$$\varphi(0) = 0 \quad \text{and} \quad \varphi(-a) = -\varphi(a) \quad (\text{for all } a \in A)$$

hold. In particular, $\text{im}(A) = \varphi(A) \subset B$ is a subgroup.

Proof Since $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$, subtraction of $\varphi(0)$ from both sides forces $0 = \varphi(0)$. The second equality is verified by the computation $\varphi(a) + \varphi(-a) = \varphi(a + (-a)) = \varphi(0) = 0$. \square

2.6.2 Kernel of a Homomorphism

For every homomorphism of abelian groups $\varphi : A \rightarrow B$, the fiber of φ over the zero element $0 \in B$ is called the *kernel* of φ and is denoted by

$$\ker \varphi \stackrel{\text{def}}{=} \varphi^{-1}(0) = \{a \in A \mid \varphi(a) = 0\}.$$

The kernel is a subgroup of A , because $\varphi(a_1) = \varphi(a_2) = 0$ implies

$$\varphi(a_1 \pm a_2) = \varphi(a_1) \pm \varphi(a_2) = 0 \pm 0 = 0.$$

Proposition 2.1 *For every homomorphism of abelian groups $\varphi : A \rightarrow B$ and every element $b = \varphi(a) \in \text{im } \varphi$,*

$$\varphi^{-1}(b) = a + \ker \varphi = \{a + a' \mid a' \in \ker \varphi\},$$

i.e., the fiber of φ over b is a shift of $\ker \varphi$ by any element $a \in \varphi^{-1}(b)$. In particular, every nonempty fiber is in bijection with $\ker \varphi$, and φ is injective if and only if $\ker \varphi = 0$.

Proof The conditions $\varphi(a_1) = \varphi(a_2)$ and $\varphi(a_1 - a_2) = 0$ are equivalent. \square

2.6.3 Group of Homomorphisms

For any two abelian groups A, B , we write $\text{Hom}(A, B)$ for the set of all homomorphisms $A \rightarrow B$. The terms monomorphism, epimorphism, and isomorphism assume on default that the map in question is a homomorphism of abelian groups. The set $\text{Hom}(A, B)$ is an abelian subgroup in the direct product B^A of A copies of the group B . The inherited group operation on homomorphisms is the pointwise addition of values:

$$\varphi_1 + \varphi_2 : a \mapsto \varphi_1(a) + \varphi_2(a).$$

Exercise 2.15 Check that the sum of homomorphisms is a homomorphism as well.

The neutral element of the group $\text{Hom}(A, B)$ is the *zero homomorphism*,¹³ which takes every element of A to the zero element of B .

2.6.4 Homomorphisms of Commutative Rings

A map of rings $\varphi : A \rightarrow B$ is called a *ring homomorphism* if it respects both operations, i.e., for all $a_1, a_2 \in A$, it satisfies the relations

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) \quad \text{and} \quad \varphi(a_1 a_2) = \varphi(a_1) \varphi(a_2). \quad (2.28)$$

Since a ring homomorphism $\varphi : A \rightarrow B$ is a homomorphism of additive groups, it possesses all the properties of homomorphisms of abelian groups. In particular, $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$, and all nonempty fibers of φ are shifts of the kernel:

$$\varphi^{-1}(\varphi(a)) = a + \ker \varphi = \{a + a' \mid a' \in \ker \varphi\},$$

where $\ker \varphi \stackrel{\text{def}}{=} \varphi^{-1}(0)$ as above. Therefore, a ring homomorphism φ is injective if and only if $\ker \varphi = \{0\}$. The kernel of a ring homomorphism has an additional property related to the multiplication. For every $a \in \ker \varphi$, all its multiples aa' also lie in $\ker \varphi$, because $\varphi(ba) = \varphi(b)\varphi(a) = 0$ for every $b \in A$. In particular, $\ker \varphi \subset A$ is a subring.

The image of a ring homomorphism $\varphi : A \rightarrow B$ is clearly a subring of B . However, a ring homomorphism does not have to respect units, and 1_B may be entirely outside $\text{im}(\varphi)$.

Exercise 2.16 Check that the map $\mathbb{Z}/(2) \rightarrow \mathbb{Z}/(6)$ sending $[0] \mapsto [0]$, $[1] \mapsto [3]$ is a ring homomorphism.

Nevertheless, every nonzero ring homomorphism to an integral domain always takes 1 to 1.

Lemma 2.5 *Let $\varphi : A \rightarrow B$ be a nonzero homomorphism of commutative rings with unit. If B has no zero divisors, then $\varphi(1) = 1$.*

Proof Since $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$, the equality $\varphi(1)(1 - \varphi(1)) = 0$ holds in the integral domain B . Hence, either $\varphi(1) = 1$ as required, or $\varphi(1) = 0$. In the latter case, $\varphi(a) = \varphi(1 \cdot a) = \varphi(1) \cdot \varphi(a) = 0$ for all $a \in A$. \square

¹³Also called the *trivial homomorphism*.

2.6.5 Homomorphisms of Fields

If commutative rings A and B are fields, then every nonzero ring homomorphism $\varphi : A \rightarrow B$ is a homomorphism of the multiplicative abelian groups $\varphi : A^* \rightarrow B^*$. In particular, $\varphi(1) = 1$ and $\varphi(a/b) = \varphi(a)/\varphi(b)$ for all a and all $b \neq 0$.

Proposition 2.2 *Every nonzero homomorphism of a field to a ring is injective.*

Proof If $\varphi(a) = 0$ for some $a \neq 0$, then $\varphi(b) = \varphi(ba^{-1}a) = \varphi(ba^{-1})\varphi(a) = 0$ for all b . Thus, a nonzero φ has zero kernel. \square

2.7 Chinese Remainder Theorem

Let any two of the numbers $n_1, n_2, \dots, n_m \in \mathbb{Z}$ be coprime and $n = n_1 n_2 \cdots n_m$. The map

$$\begin{aligned} \varphi : \mathbb{Z}/(n) &\rightarrow (\mathbb{Z}/(n_1)) \times (\mathbb{Z}/(n_2)) \times \cdots \times (\mathbb{Z}/(n_m)) \\ [z]_n &\mapsto ([z]_{n_1}, [z]_{n_2}, \dots, [z]_{n_m}), \end{aligned} \tag{2.29}$$

which takes the residue class $z \pmod{n}$ to the collection of residue classes $z \pmod{n_i}$, is well defined, because for every $z_1 \equiv z_2 \pmod{n}$, the difference $z_1 - z_2$ is a multiple of $n = n_1 n_2 \cdots n_m$, and therefore $[z_1]_{n_i} = [z_2]_{n_i}$ for all i . It follows from the computation

$$\begin{aligned} \varphi([z]_n + [w]_n) &= \varphi([z + w]_n) = ([z + w]_{n_1}, [z + w]_{n_2}, \dots, [z + w]_{n_m}) \\ &= ([z]_{n_1} + [w]_{n_1}, [z]_{n_2} + [w]_{n_2}, \dots, [z]_{n_m} + [w]_{n_m}) \\ &= ([z]_{n_1}, [z]_{n_2}, \dots, [z]_{n_m}) + ([w]_{n_1}, [w]_{n_2}, \dots, [w]_{n_m}) \\ &= \varphi([z]_n) + \varphi([w]_n) \end{aligned}$$

that φ respects the addition. A similar calculation verifies that φ respects the multiplication as well. Therefore, the map (2.29) is a ring homomorphism. By Lemma 2.3 on p. 26, every $z \in \mathbb{Z}$ such that $[z]_{n_i} = 0$ for all i is divisible by $n = n_1 \cdot n_2 \cdots n_m$. Hence, φ is injective. Since the cardinalities of both sets $\mathbb{Z}/(n)$, $\prod \mathbb{Z}/(n_i)$ are equal to $n = \prod n_i$, the homomorphism (2.29) is bijective. This fact is known as the *Chinese remainder theorem*. In ordinary language, it says that for every collection of remainders r_1, r_2, \dots, r_m under division by pairwise coprime numbers $n_1, n_2, \dots, n_m \in \mathbb{N}$, there exists a number $z \in \mathbb{Z}$ whose remainder on division by n_i is r_i simultaneously for all i , and two numbers z_1, z_2 sharing this property differ by a multiple of $n = n_1 n_2 \cdots n_k$.

A practical computation of such a number z can be done by means of the Euclidean algorithm as follows. By Lemma 2.3 on p. 26, each n_i is coprime to the product $m_i = \prod_{v \neq i} n_v$ of all the other n_v 's. Therefore, the Euclidean algorithm allows us to find for each i some $x_i, y_i \in \mathbb{Z}$ such that $n_i x_i + m_i y_i = 1$. Then $b_i = m_i y_i$ is congruent to 1 modulo n_i and to 0 modulo all the other n_v 's. Hence, $z = r_1 b_1 + r_2 b_2 + \cdots + r_m b_m$ solves the problem.

Example 2.7 To demonstrate the effectiveness of the above procedure, let us find the smallest positive integer with remainders $r_1 = 2, r_2 = 7, r_3 = 43$ on division by $n_1 = 57, n_2 = 91, n_3 = 179$ respectively.¹⁴ We first invert $91 \cdot 179$ modulo 57. Since $91 \cdot 179 \equiv 34 \cdot 8 \equiv -13 \pmod{57}$, we can apply the Euclidean algorithm to $E_0 = 57, E_1 = 13$. The output $22 \cdot 13 - 5 \cdot 57 = 1$ (check!) means that $-22 \cdot 91 \cdot 179 \equiv 1 \pmod{57}$. Thus, the number

$$b_1 = -22 \cdot 91 \cdot 179 \quad (\equiv 22 \cdot 13 \pmod{57})$$

produces the remainder triple $(1, 0, 0)$ on division by 57, 91, 179. Similarly, we obtain the numbers

$$b_2 = -33 \cdot 57 \cdot 179 \quad (\equiv 33 \cdot 11 \pmod{91}),$$

$$b_3 = -45 \cdot 57 \cdot 91 \quad (\equiv 45 \cdot 4 \pmod{179}),$$

producing the remainder triples $(0, 1, 0)$ and $(0, 0, 1)$ on division by 57, 91, 179. The required remainders $(2, 7, 43)$ are produced by

$$\begin{aligned} z = 2b_1 + 7b_2 + 43b_3 &= -(2 \cdot 22 \cdot 91 \cdot 179 + 7 \cdot 33 \cdot 57 \cdot 179 + 43 \cdot 45 \cdot 57 \cdot 91) \\ &= -(716\,716 + 2\,356\,893 + 10\,036\,845) = -13\,110\,454, \end{aligned}$$

as well as by all numbers that differ from z by a multiple of $n = 57 \cdot 91 \cdot 179 = 928\,473$. The smallest positive among them is equal to $z + 15n = 816\,641$.

2.8 Characteristic

2.8.1 Prime Subfield

For a commutative ring K with unit there is a ring homomorphism $\kappa : \mathbb{Z} \rightarrow K$ defined by

$$\kappa(\pm n) = \pm \underbrace{(1 + 1 + \cdots + 1)}_n \text{ for all } n \in \mathbb{N}. \quad (2.30)$$

¹⁴2, 7, 43, 57, 91, and 179 are the numbers of famous mathematical schools in Moscow.

Its image $\text{im } \kappa \subset K$ coincides with the intersection of all subrings in K containing the unit element of K . If κ is injective, we say that K has *zero characteristic* and write $\text{char } K = 0$. Otherwise, we say that K has *positive characteristic* and define the *characteristic* $\text{char } K$ to be the minimal $m \in \mathbb{N}$ such that $\underbrace{1 + 1 + \cdots + 1}_m = 0$.

The equality

$$\underbrace{1 + 1 + \cdots + 1}_{mn} = \underbrace{(1 + 1 + \cdots + 1)}_m \cdot \underbrace{(1 + 1 + \cdots + 1)}_n$$

implies that the characteristic of an integral domain is either zero or a *prime* number $p \in \mathbb{N}$. For an integral domain K of positive characteristic p , the homomorphism (2.30) takes all multiples of p to zero and therefore can be factorized into the composition $\kappa_p \circ \pi_p$ of ring homomorphisms

$$\pi_p : \mathbb{Z} \twoheadrightarrow \mathbb{F}_p, z \mapsto [z]_p \quad \text{and} \quad \kappa_p : \mathbb{F}_p \hookrightarrow K, [z]_p \mapsto \kappa(z), \quad (2.31)$$

the latter of which is injective by Proposition 2.2 on p. 34, because \mathbb{F}_p is a field. Thus, the smallest subring with unit in an integral domain K of positive characteristic p is a field isomorphic to $\mathbb{F}_p = \mathbb{Z}/(p)$. It is called the *prime subfield* of K .

For a field \mathbb{F} , the *prime subfield* of \mathbb{F} is defined to be the intersection of all subfields in \mathbb{F} . This is the smallest subfield in \mathbb{F} with respect to inclusion. Clearly, it contains $\text{im}(\kappa)$. If $\text{char}(\mathbb{F}) = p > 0$, then the previous arguments force the prime subfield to be equal to $\text{im } \kappa = \text{im}(\kappa_p) \simeq \mathbb{Z}/(p)$. Thus, our second definition of the prime subfield agrees with the previous one in this case.

For a field \mathbb{F} of zero characteristic, the homomorphism $\kappa : \mathbb{Z} \hookrightarrow \mathbb{F}$ is injective. Since all nonzero elements in $\text{im } \kappa$ are invertible within \mathbb{F} , the assignment

$$p/q \mapsto \kappa(p)/\kappa(q)$$

extends κ to a homomorphism of fields $\tilde{\kappa} : \mathbb{Q} \hookrightarrow \mathbb{F}$, which is injective by Proposition 2.2 on p. 34. We conclude that the prime subfield of \mathbb{F} coincides with $\text{im } \tilde{\kappa}$ and is isomorphic to \mathbb{Q} in this case.

Exercise 2.17 Show that (a) every field endomorphism leaves every element in the prime field fixed; (b) there are no nonzero homomorphisms whatever between fields of different characteristics.

In particular, the field \mathbb{Q} is pointwise fixed by every automorphisms of the fields \mathbb{R} and \mathbb{C} .

2.8.2 Frobenius Endomorphism

The same arguments as in Example 2.6 on p. 29 show that for a field \mathbb{F} of characteristic $p > 0$, the p -power exponentiation

$$F_p : \mathbb{F} \rightarrow \mathbb{F}, \quad x \mapsto x^p, \quad (2.32)$$

is a ring homomorphism, because $(ab)^p = a^p b^p$ and

$$(a + b)^p = a^p + b^p + \sum_{k=1}^{p-1} \underbrace{(1 + 1 + \cdots + 1)}_{\binom{p}{k}} \cdot a^k b^{p-k} = a^p + b^p.$$

The homomorphism (2.32) is called the *Frobenius endomorphism* or just the *Frobenius* for short. The previous exercise, [Exercise 2.17](#), says that the Frobenius acts identically on the prime subfield $\mathbb{F}_p \subset \mathbb{F}$. This agrees with Fermat's little theorem, Theorem 2.1 on p. 30.

Exercise 2.18 Show that a field \mathbb{F} of characteristic $p > 0$ is isomorphic to \mathbb{F}_p if and only if the Frobenius endomorphism $F_p : \mathbb{F} \rightarrow \mathbb{F}$ coincides with the identity map $\text{Id}_{\mathbb{F}}$.

Problems for Independent Solution to Chap. 2

Problem 2.1 Compute $\text{GCD}(a, b)$ and express it as $ax + by$ with $x, y \in \mathbb{Z}$ for the following pairs (a, b) : **(a)** $(17, 13)$, **(b)** $(44\,863, 70\,499)$, **(c)** $(8\,385\,403, 2\,442\,778)$.

Problem 2.2 Find all integer solutions of the following equations: **(a)** $5x + 7y = 11$, **(b)** $26x + 32y = 60$, **(c)** $1537x + 1387y = 1$, **(d)** $169x + 221y = 26$, **(e)** $28x + 30y + 31z = 365$.

Problem 2.3 Find the ninety-first positive integer that has remainders: **(a)** 2 and 7 on division by 57 and 179, **(b)** 1, 2, 3 on division by 2, 3, 5, **(c)** 2, 4, 6, 8 on division by 5, 9, 11, 14.

Problem 2.4 How many solutions does the equation $x^2 = 1$ have in the ring $\mathbb{Z}/(n)$ for even $n \geq 4$?

Problem 2.5 Prove that for each $m \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that the equation $x^2 = 1$ has at least m solutions in $\mathbb{Z}/(n)$.

Problem 2.6 How many solutions does the equation **(a)** $x^3 = 1$, **(b)** $x^2 = 49$, have in the ring $\mathbb{Z}/(360)$?

Problem 2.7 For each ring $\mathbb{Z}/(m)$ in the range $4 \leq m \leq 8$, write the multiplication table and list all the squares, all the nilpotents, all the zero divisors, and all the invertible elements. For each invertible element, indicate its inverse.

Problem 2.8 Show that: **(a)** $a^2 + b^2 : 7 \Rightarrow a : 7$ and $b : 7$, **(b)** $a^3 + b^3 + c^3 : 7 \Rightarrow abc : 7$, **(c)** $a^2 + b^2 + c^2 + d^2 + e^2 : 9 \Rightarrow abcde : 9$.

Problem 2.9 Does the equation $x^2 + y^2 + z^2 = 2xyz$ have any integer solutions besides $(0, 0, 0)$?

Problem 2.10 Fix some nonzero $a \in \mathbb{Z}/(n)$ and write $\alpha : \mathbb{Z}/(n) \rightarrow \mathbb{Z}/(n)$, $x \mapsto ax$, for the multiplication-by- a map. Prove that the following conditions

are equivalent: **(a)** a is invertible; **(b)** a is not a zero divisor; **(c)** α is injective; **(d)** α is surjective; **(e)** α is bijective.

Problem 2.11 (Euler's Theorem on Residues) Let $a \in \mathbb{Z}/(n)$ satisfy the conditions of the previous problem. Depict all elements of $\mathbb{Z}/(n)$ by some points on a sheet of paper and for each point x , draw an arrow from x to ax . Prove that in this picture:

- (a) movement along the arrows decomposes into disjoint nonintersecting cycles;
- (b) if a cycle goes through an invertible element, then all the elements it goes through are invertible;
- (c) all cycles passing through invertible elements are of the same length;
- (d) $a^{\varphi(n)} = 1$, where $\varphi(n)$ is the Euler function defined in Sect. 2.4.3 on p. 28.

Problem 2.12 Are $2222^{5555} + 5555^{2222}$ and $2^{70} + 3^{70}$ divisible by 7 and 13 respectively?

Problem 2.13 Find remainder on division of $2015^{2016^{2017}}$ by 11.

Problem 2.14 For all $k \in \mathbb{N}$, find the remainders on division of 10^k by 2, 5, 4, 3, 9, 11, 7, 13. Formulate and prove algorithms¹⁵ to calculate the remainder on division of a given decimal number d by 2, 5, 4, 3, 9, 11, 7, 13 by looking at the digits of d .¹⁶

Problem 2.15 (Primitive Invertible Residue Classes) Let $a \in \mathbb{Z}/(n)^*$ be an invertible residue class. The minimal $k \in \mathbb{N}$ such that $a^k = 1$ is called the *order* of a . We say that a *generates* the multiplicative group $\mathbb{Z}/(n)^*$ if this group is exhausted by the integer powers a^k . The generators of $\mathbb{Z}/(n)^*$ are also called *primitive roots* (or *primitive residues*) modulo n . Show that an invertible residue a is primitive if and only if the order of a equals $\varphi(n)$.

- (a) Prove the existence of a primitive residue modulo p for every prime $p \in \mathbb{N}$.
- (b) Let $a_1, a_2, \dots, a_n \in \mathbb{Z}/(n)^*$ have pairwise coprime orders k_1, k_2, \dots, k_n . Find the order of the product $a_1 \cdots a_n$.
- (c) For two arbitrary invertible residues a, b of arbitrary orders k, m , construct an invertible residue of order $\text{LCM}(k, m)$.
- (d) Fix a prime $p > 2$ and a primitive residue q modulo p . Show that there exists $\vartheta \in \mathbb{N}$ such that: (1) $(q + p\vartheta)^{p-1} \equiv 1 \pmod{p}$; (2) $(q + p\vartheta)^{p-1} \not\equiv 1 \pmod{p^2}$; (3) the class $[q + p\vartheta]$ is a primitive residue class modulo p^k for all $k \in \mathbb{N}$.
- (e) For $k \in \mathbb{N}$ and prime $p > 2$, prove the existence of a primitive residue modulo $2p^k$.
- (f) Is there a primitive residue modulo 21?

¹⁵Try to make them as simple as possible.

¹⁶For example, the remainder on division by 3 is equal to the remainder of the sum of the digits.

Problem 2.16 (Idempotents) An element a of an arbitrary commutative ring with unit is called *idempotent* if $a^2 = a$. The idempotents 0 and 1 are called *trivial*. Show that (a) each nontrivial idempotent is a zero divisor; (b) a is idempotent if and only if $1 - a$ is too. (c) For which n are there nontrivial idempotents in $\mathbb{Z}/(n)$?

Problem 2.17 Find all idempotents in the ring $\mathbb{Z}/(n)$ for (a) $n = 6$, (b) $n = 36$, (c) $n = p_1 p_2 \cdots p_n$, (d) $n = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$, where p_i are distinct prime numbers.

Problem 2.18 (Euler's Formula for φ) A function $f : \mathbb{N} \rightarrow \mathbb{C}$ is called a *multiplicative character* if $f(mn) = f(m)f(n)$ for every coprime $m, n \in \mathbb{Z}$. Show that Euler's function¹⁷ φ is a multiplicative character and for every $n = p_1^{m_1} \cdots p_n^{m_n}$, where p_i are distinct primes, prove Euler's formula

$$\varphi(n) = n \cdot (1 - p_1^{-1}) \cdots (1 - p_n^{-1}).$$

Find all $n \in \mathbb{N}$ such that $\varphi(n) = 10$.

Problem 2.19 (Möbius Function) The Möbius function $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$ gives $\mu(1) = 1$ and $\mu(n) = 0$ for all n divisible by the square of some prime number. Otherwise, $\mu(n) = (-1)^s$, where s is the number of positive prime divisors of n . Show that μ is a multiplicative character and prove the equality

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{for } n = 1, \\ 0 & \text{for } n > 1, \end{cases}$$

where the summation runs through all divisors of n including $d = 1, n$.

Problem 2.20 (Möbius Inversion Formula) Given a function $g : \mathbb{N} \rightarrow \mathbb{C}$, define a new function $\sigma_g : \mathbb{N} \rightarrow \mathbb{C}$ by $\sigma_g(n) = \sum_{d|n} g(d)$. Prove that g is recovered from σ_g as $g(n) = \sum_{d|n} \sigma(d) \cdot \mu(n/d)$.

Problem 2.21 For each $m \in \mathbb{N}$, evaluate $\sum_{d|m} \varphi(d)$, where φ is Euler's function.

Problem 2.22 (Wilson's Theorem) Solve the quadratic equation $x^2 = 1$ in the field \mathbb{F}_p and evaluate the product of all nonzero elements of \mathbb{F}_p . Deduce from this computation that an integer $p \geq 2$ is prime if and only if $p \mid (p-1)! + 1$.

Problem 2.23 Describe the sets of all values of polynomials (a) $x^p - x$, (b) x^{p-1} , (c) $x^{\frac{p-1}{2}}$, for x running through \mathbb{F}_p and for x running through the set of all squares in \mathbb{F}_p .

Problem 2.24 How many nonzero squares are there in \mathbb{F}_p ? Show that the equation $x^2 + y^2 = -1$ is solvable in $x, y \in \mathbb{F}_p$ for every prime $p > 2$.

¹⁷See Sect. 2.4.3 on p. 28.

Problem 2.25 (Gauss's Lemma) Write all elements of \mathbb{F}_p in order as

$$-[(p-1)/2], \dots, -[1], [0], [1], \dots, [(p-1)/2].$$

Prove that $a \in \mathbb{F}_p^*$ is a square if and only if an even number of “positive” elements become “negative” under multiplication by a .

Problem 2.26 For what primes p is the equation **(a)** $x^2 = -1$, **(b)** $x^2 = 2$, solvable in \mathbb{F}_p ?¹⁸

¹⁸ ANSWERS: In **(a)** for $p = 2$ and $p \equiv 1 \pmod{4}$; in **(b)** if and only if $(p^2 - 1)/8$ is even.

Chapter 3

Polynomials and Simple Field Extensions

In this chapter, K will denote an arbitrary commutative ring with unit and \mathbb{k} an arbitrary field.

3.1 Formal Power Series

3.1.1 Rings of Formal Power Series

Given an infinite sequence of elements $a_i \in K$, $i \geq 0$, an expression of the form

$$f(x) = \sum_{v \geq 0} a_v x^v = a_0 + a_1 x + a_2 x^2 + \cdots \quad (3.1)$$

is called a *formal power series* in the variable x with coefficients in K . Two power series

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots \quad \text{and} \quad g(x) = b_0 + b_1 x + b_2 x^2 + \cdots \quad (3.2)$$

are *equal* if $a_i = b_i$ for all i . Formal power series (3.2) are added and multiplied by the usual rules for multiplying out and collecting like terms. Namely, the coefficients of the series

$$f(x) + g(x) = s_0 + s_1 x + s_2 x^2 + \cdots \quad \text{and} \quad f(x)g(x) = p_0 + p_1 x + p_2 x^2 + \cdots$$

are defined by¹

$$s_m \stackrel{\text{def}}{=} a_m + b_m, \quad p_m \stackrel{\text{def}}{=} \sum_{\alpha+\beta=m} a_\alpha b_\beta = a_0 b_m + a_1 b_{m-1} + \cdots + a_m b_0. \quad (3.3)$$

Exercise 3.1 Check that these operations satisfy the axioms of a commutative ring.

We write $K[[x]]$ for the ring of power series in x with coefficients in K . The initial coefficient a_0 in (3.1) is called the *constant term* of f . The leftmost summand with nonzero coefficient in (3.1) is called the *lowest term* of f . Its power and coefficient are called the *lowest degree* and *lowest coefficient* of f . If K has no zero divisors, then the lowest term in a product of power series is equal to the product of the lowest terms of the factors. Hence, if K is an integral domain, then $K[[x]]$ is an integral domain too.

The ring $K[[x_1, x_2, \dots, x_n]]$ of power series in n variables is defined by induction:

$$K[[x_1, x_2, \dots, x_n]] \stackrel{\text{def}}{=} K[[x_1, x_2, \dots, x_{n-1}]] [[x_n]].$$

It consists of infinite sums of the type $\sum a_{v_1 \dots v_n} x_1^{v_1} x_2^{v_2} \cdots x_n^{v_n}$, where the v_i run independently through nonnegative integers and $a_{v_1 \dots v_n} \in K$.

3.1.2 Algebraic Operations on Power Series

An n -ary operation on $K[[x]]$ is a map of sets

$$\underbrace{K[[x]] \times K[[x]] \times \cdots \times K[[x]]}_n \rightarrow K[[x]]$$

sending an n -tuple of series $f_1, f_2, \dots, f_n \in K[[x]]$ to a new series f depending on f_1, f_2, \dots, f_n . Such an operation is called *algebraic* if every coefficient of f can be evaluated by a finite number of additions, subtractions, multiplications, and well-defined divisions applied to a finite number of coefficients of the f_i .

For example, the addition and multiplication defined in (3.3) are algebraic binary operations, whereas the evaluation of f at some point $x = \alpha \in K$ is not algebraic in most cases, because it usually requires infinitely many additions and multiplications. However, there is an important evaluation that always can be done, the evaluation at zero, which takes $f(0) = a_0$.

¹Formally speaking, these rules define addition and multiplication of *sequences* (a_v) , (b_v) formed by elements of K . The variable x is used only to simplify the visual perception of these operations.

For a power series $g(x) = b_1x + b_2x^2 + \dots$ without constant term, an important unary algebraic operation is provided by the substitution $x \leftarrow g(x)$, which takes $f(x) \in K[[x]]$ to

$$\begin{aligned} f(g(x)) &= \sum a_k(b_1x + b_2x^2 + \dots)^k \\ &= a_0 + a_1(b_1x + b_2x^2 + \dots) + a_2(b_1x + b_2x^2 + \dots)^2 + a_3(b_1x + b_2x^2 + \dots)^3 \\ &\quad + \dots \\ &= a_0 + (a_1b_1) \cdot x + (a_1b_2 + a_2b_1^2) \cdot x^2 + (a_1b_3 + 2a_2b_1b_2 + a_3b_1^3) \cdot x^3 + \dots, \end{aligned}$$

whose coefficient at x^m depends only on the first m terms of f .

Proposition 3.1 *A power series $f(x) = a_0 + a_1x + a_2x^2 + \dots \in K[[x]]$ is invertible in $K[[x]]$ if and only if its constant term $a_0 \in K$ is invertible in K . The inversion map $f \mapsto f^{-1}$ is a unary algebraic operation on the multiplicative group $K[[x]]^*$ of invertible power series.*

Proof If there exists $f^{-1}(x) = b_0 + b_1x + b_2x^2 + \dots$ such that $f(x) \cdot f^{-1}(x) = 1$, then $a_0b_0 = 1$, i.e., a_0 is invertible. Conversely, let $a_0 \in K$ be invertible. A comparison of coefficients at the same power of x on both sides of

$$(a_0 + a_1x + a_2x^2 + \dots) \cdot (b_0 + b_1x + b_2x^2 + \dots) = 1$$

leads to an infinite system of equations in the b_i :

$$\begin{aligned} a_0b_0 &= 1, \\ a_0b_1 + a_1b_0 &= 0, \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0, \\ &\dots \end{aligned} \tag{3.4}$$

from which we obtain $b_0 = a_0^{-1}$ and $b_k = -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \dots + a_kb_0)$ for $k \geq 1$. \square

Exercise 3.2 In $\mathbb{Q}[[x]]$ compute $(1-x)^{-1}$, $(1-x^2)^{-1}$, and $(1-x)^{-2}$.

3.1.3 Polynomials

A power series that has only a finite number of nonzero coefficients is called a *polynomial*. The set of polynomials in the variables x_1, x_2, \dots, x_n form a ring,

denoted by

$$K[x_1, x_2, \dots, x_n] \subset K[[x_1, x_2, \dots, x_n]].$$

A polynomial in one variable x is a finite sum $f(x) = a_0 + a_1x + \dots + a_nx^n$. The rightmost nonzero term a_nx^n and its coefficient $a_n \neq 0$ are called the *leading term* and coefficient in f . A polynomial with leading coefficient 1 is called *reduced* or *monic*. The leading exponent n is called the *degree* of f and is denoted by $\deg f$. Polynomials of degree zero are exactly the nonzero constants. It is convenient to put $\deg 0 \stackrel{\text{def}}{=} -\infty$. If K has no zero divisors, then the leading term of a product f_1f_2 equals the product of the leading terms of f_1, f_2 . Hence, $\deg(f_1f_2) = \deg f_1 + \deg f_2$ over such a K . In particular, $K[x]$ is an integral domain, and the invertible elements in $K[x]$ are exhausted by the invertible constants.

Exercise 3.3 Check that $y - x$ divides $y^n - x^n$ in $\mathbb{Z}[x, y]$ and compute the quotient.

3.1.4 Differential Calculus

Substitution of $x + t$ for x in a power series

$$f(x) = a_0 + a_1x + a_2x^2 + \dots$$

gives a power series in the two variables x, t :

$$f(x + t) = a_0 + a_1(x + t) + a_2(x + t)^2 + \dots.$$

Let us expand and collect terms of the same power in t :

$$f(x + t) = f_0(x) + f_1(x) \cdot t + f_2(x) \cdot t^2 + f_3(x) \cdot t^3 + \dots = \sum_{m \geq 0} f_m(x) \cdot t^m. \quad (3.5)$$

This is a power series in t with coefficients $f_m \in K[[x]]$, which are uniquely determined by f and depend algebraically on f in the sense of Sect. 3.1.2.

Exercise 3.4 Check that $f_0(x) = f(x)$.

The series $f_1(x)$ in (3.5) is called the *derivative* of f and is denoted by f' or by $\frac{d}{dx}f$. It is uniquely determined by the condition

$$f(x + t) = f(x) + f'(x) \cdot t + (\text{terms divisible by } t^2) \quad \text{in } K[[x, t]]. \quad (3.6)$$

By [Exercise 3.3](#), the difference $f(x+t)-f(x)$ is divisible by t in $K[[x, t]]$. The constant term of the quotient

$$\begin{aligned} \frac{f(x+t)-f(x)}{t} &= a_1 \cdot \frac{(x+t)-t}{t} + a_2 \cdot \frac{(x+t)^2-t^2}{t} + a_3 \cdot \frac{(x+t)^3-t^3}{t} + \dots \\ &= \sum_{k \geq 1} a_k \cdot ((x+t)^{k-1} + (x+t)^{k-2}x + (x+t)^{k-3}x^2 + \dots + x^{k-1}) \end{aligned}$$

can be obtained by evaluation at $t = 0$. This leads to the well-known formula

$$f'(x) = \sum_{k \geq 1} k a_k x^{k-1} = a_1 + 2 a_2 x + 3 a_3 x^2 + \dots, \quad (3.7)$$

where each multiplier k in front of $a_k x^{k-1}$ means the sum of k unit elements in K . Note that everything just said makes sense over any commutative ring K with unit.

Example 3.1 (Series with Zero Derivative) Now assume that K is an integral domain. If the characteristic² $\text{char } K$ is equal to 0, then formula (3.7) implies that $f' = 0$ if and only if $f = \text{const}$. However, if $\text{char } K = p > 0$, the derivation kills exactly all the monomials x^m whose degree m is divisible by p . Thus, for power series with coefficients in an integral domain K of characteristic $p > 0$, the condition $f'(x) = 0$ means that $f(x) = g(x^p)$ for some $g \in K[[x]]$. Moreover, the same is true in the subring of polynomials $K[x] \subset K[[x]]$.

Lemma 3.1 *Over any prime $p \in \mathbb{N}$, the polynomials with zero derivative in $\mathbb{F}_p[x]$ are exhausted by the p th powers g^p , $g \in \mathbb{F}_p[x]$.*

Proof Since the Frobenius endomorphism³ $F_p : \mathbb{F}_p[x] \rightarrow \mathbb{F}_p[x]$, $h \mapsto h^p$, acts identically on the coefficients, for every $g(x) = b_0 x^m + b_1 x^{m-1} + \dots + b_{m-1} x + b_m \in \mathbb{F}_p[x]$, we have

$$\begin{aligned} g(x^p) &= b_0 x^{pm} + b_1 x^{p(m-1)} + \dots + b_{m-1} x^p + b_m \\ &= b_0^p x^{pm} + b_1^p x^{p(m-1)} + \dots + b_{m-1}^p x^p + b_m^p \\ &= (b_0 x^m + b_1 x^{m-1} + \dots + b_{m-1} x + b_m)^p = g^p(x). \end{aligned}$$

□

Proposition 3.2 (Differentiation Rules) *For a commutative ring K with unit, the following equalities hold:*

$$(\alpha f)' = \alpha \cdot f' \quad \text{for every } \alpha \in K \text{ and } f, g \in K[[x]], \quad (3.8)$$

$$(f + g)' = f' + g' \quad \text{for every } f, g \in K[[x]], \quad (3.9)$$

²See Sect. 2.8 on p. 35.

³See Sect. 2.8.2 on p. 36.

$$(fg)' = f' \cdot g + f \cdot g' \quad \text{for every } f, g \in K[x], \quad (3.10)$$

$$(f(g(x)))' = g'(x) \cdot f'(g(x)) \quad \text{for all } f \text{ and all } g \text{ with no constant term}, \quad (3.11)$$

$$(f^{-1})' = -f'/f^2 \quad \text{for every invertible } f \in K[x]. \quad (3.12)$$

Proof The first two equalities follow directly from (3.7). To verify the *Leibniz rule* (3.10), write

$$f(x+t) = f(x) + t \cdot f'(x) + (\text{terms divisible by } t^2),$$

$$g(x+t) = g(x) + t \cdot g'(x) + (\text{terms divisible by } t^2).$$

Then $f(x+t)g(x+t) = f(x)g(x) + t \cdot (f'(x)g(x) + f(x)g'(x)) + (\text{terms divisible by } t^2)$. By (3.6), this means that $(fg)' = f' \cdot g + f \cdot g'$. The equality (3.11) is proved in a similar way. Let $\tau(x, t) = g(x+t) - g(x) = t \cdot g'(x) + (\text{terms divisible by } t^2)$. Then

$$\begin{aligned} f(g(x+t)) &= f(g(x) + \tau(x, t)) \\ &= f(g(x)) + \tau(x, t) \cdot f'(g(x)) + (\text{terms divisible by } \tau(x, t)^2) \\ &= f(g(x)) + t \cdot g'(x) \cdot f'(g(x)) + (\text{terms divisible by } t^2). \end{aligned}$$

Therefore $(f(g(x)))' = g'(x) \cdot f'(g(x))$ by (3.6). Equality (3.12) is verified by the differentiation of both sides of the equality $f \cdot f^{-1} = 1$. This gives $f' \cdot f^{-1} + f \cdot (f^{-1})' = 0$ and forces $(f^{-1})' = -f'/f^2$. \square

Exercise 3.5 For $m \in \mathbb{N}$, show that $f_m = \frac{1}{m!} \frac{d^m}{dx^m} f(x)$ in formula (3.5) on p. 44. Here we write $\frac{d^m}{dx^m} = \left(\frac{d}{dx}\right)^m$ for the m -fold derivation map $\frac{d}{dx} : f \mapsto f'$.

3.2 Polynomial Rings

3.2.1 Division

Perhaps you learned how to carry out polynomial long division in school. It is similar to the long division of integers and is applicable in a number of mathematical situations.

Proposition 3.3 (Division with Remainder) *Let K be a commutative ring with unit and $u \in K[x]$ a polynomial with invertible leading coefficient. Then for a given polynomial $f \in K[x]$, there exist polynomials $q, r \in K[x]$ such that $f = u \cdot q + r$, and either $\deg(r) < \deg(u)$ or $r = 0$. If K has no zero divisors, then q and r are uniquely determined by f and u .*

Proof Let $u = b_0x^k + b_1x^{k-1} + \cdots + b_{k-1}x + b_k$. If $\deg f < k$, we can take $q = 0$, $r = f$. For $f = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$, where $n \geq k$, assume inductively that q and r exist for all polynomials f of degree $\deg f < n$. Since the difference $f - a_0b_0^{-1}x^{n-k}u$ has degree less than n , it can be written as $qu + r$, where either $r = 0$ or $\deg r < k$. Then $f = (q + a_0b_0^{-1}x^{n-k}) \cdot u + r$ also has such a form. Now let K be an integral domain and let p, s be another pair of polynomials such that $\deg(s) < k$ and $up + s = f = uq + r$. Then $u(q - p) = r - s$. If $p - q \neq 0$, then the left-hand side has degree at least k , whereas the degree of the right-hand side is strictly less than k . Thus, $p - q = 0$, and therefore $r - s = 0$. \square

Definition 3.1 The polynomials q and r from Proposition 3.3 are called the *quotient* and *remainder* on division of f by u in $K[x]$.

Example 3.2 (Evaluation of a Polynomial) For a polynomial $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in K[x]$, the remainder on division of f by a linear binomial $x - \alpha$ has degree at most zero, i.e., is a constant. Substitution of $x = \alpha$ in the equality $f(x) = (x - \alpha) \cdot q(x) + r$ leads to $r = f(\alpha)$. Thus, the *value* of f at $\alpha \in K$ is equal to the remainder on division of f by $x - \alpha$. Note that calculation of $f(\alpha)$ by the long division algorithm is much faster than simply evaluating all powers α^m and then adding them together.

Exercise 3.6 (Horner's Method) Check that

$$f(\alpha) = a_0 + \alpha \cdot \left(a_1 + \alpha \cdot \left(a_2 + \cdots + \alpha \cdot \left(a_{n-2} + \alpha \cdot (a_{n-1} + \alpha \cdot a_n) \right) \cdots \right) \right).$$

Corollary 3.1 For a field \mathbb{k} and two polynomials $f, g \in \mathbb{k}[x]$, there exists a unique pair of polynomials $q, r \in \mathbb{k}[x]$ such that $f = g \cdot q + r$ and either $\deg(r) < \deg(g)$ or $r = 0$. \square

Proposition 3.4 For a field \mathbb{k} and collection of polynomials $f_1, f_2, \dots, f_n \in \mathbb{k}[x]$, there exists a unique monic polynomial $d \in \mathbb{k}[x]$ dividing all f_i and divisible by every common divisor of all the f_i . Moreover, this polynomial d can be written as

$$f_1h_1 + f_2h_2 + \cdots + f_nh_n \text{ where } h_i \in \mathbb{k}[x]. \quad (3.13)$$

A polynomial $g \in \mathbb{k}[x]$ can be represented in the form (3.13) if and only if $d \mid g$.

Proof Existence is established by the same arguments as in Sect. 2.4.3 on p. 28. Write

$$(f_1, f_2, \dots, f_n) \stackrel{\text{def}}{=} \{f_1h_1 + f_2h_2 + \cdots + f_nh_n \mid h_i \in \mathbb{k}[x]\} \quad (3.14)$$

for the set of all polynomials representable in the form (3.13). This is a subring of $\mathbb{k}[x]$ such that $g \in (f_1, f_2, \dots, f_n)$ forces $hg \in (f_1, f_2, \dots, f_n)$ for all $h \in \mathbb{k}[x]$. Note that $f_i \in (f_1, f_2, \dots, f_n)$ for all i , every element of (f_1, f_2, \dots, f_n) is divisible by every

common divisor of all the f_i , and every polynomial in (f_1, f_2, \dots, f_n) can be made monic by multiplying by the constant inverse of its leading coefficient. Write d for any monic polynomial of lowest degree in (f_1, f_2, \dots, f_n) . It is enough to check that d divides every $g \in (f_1, f_2, \dots, f_n)$. The remainder $r = g - qd \in (f_1, f_2, \dots, f_n)$ on such a division either has $\deg r < \deg d$ or vanishes. The first is impossible by the choice of d .

To prove uniqueness, note that given two polynomials d_1, d_2 such that $d_1 \mid d_2$ and $d_2 \mid d_1$, then $\deg d_1 = \deg d_2$ and $d_1/d_2 = \text{const}$. If both polynomials are monic, the constant has to be 1, whence the choice of d is unique. \square

Definition 3.2 The polynomial d from Proposition 3.4 is called the *greatest common divisor* of the polynomials f_i and is denoted by $\text{GCD}(f_1, f_2, \dots, f_n)$.

3.2.2 Coprime Polynomials

By Proposition 3.4, the polynomials $f_1, f_2, \dots, f_m \in \mathbb{k}[x]$ are *coprime*⁴ if and only if they have no common divisors except for constants. This is similar to what we had in the ring of integers, and for this reason, $\mathbb{k}[x]$ and \mathbb{Z} share a number of very nice divisibility properties.

Definition 3.3 (Reducibility) Let K be an arbitrary commutative ring with unit. An element $f \in K$ is called *reducible* if $f = gh$ for some noninvertible $g, h \in K$. Note that all reducible elements are noninvertible. Noninvertible nonreducible elements are called *irreducible*.

For example, a polynomial $f \in \mathbb{k}[x]$ is reducible in $\mathbb{k}[x]$ if and only if $f = gh$ for some $g, h \in \mathbb{k}[x]$ such that $\deg g < \deg f$ and $\deg h < \deg f$.

Exercise 3.7 Let \mathbb{k} be a field. Show that $q \in \mathbb{k}[x]$ is irreducible if and only if $\text{GCD}(d, f) = 1$ for all $f \in \mathbb{k}[x]$ such that $\deg f < \deg q$. Use Lemma 2.3 on p. 26 to prove the *factorization theorem* for $\mathbb{k}[x]$: each $f \in \mathbb{Z}$ is equal to a finite product of irreducible polynomials, and two such factorizations $p_1 p_2 \cdots p_k = f = q_1 q_2 \cdots q_m$ have $k = m$ and (after appropriate renumbering of factors) $p_i = \lambda_i \cdot q_i$ for all i and some $\lambda_i \in \mathbb{k}$.

3.2.3 Euclidean Algorithm

We may translate the Euclidean algorithm from Sect. 2.2.3 on p. 25 word for word into the context of $\mathbb{k}[x]$. Given two polynomials $f_1, f_2 \in \mathbb{k}[x]$ with $\deg(f_1) \geq \deg(f_2)$,

⁴By definition, this means that $1 = h_1 f_1 + h_2 f_2 + \cdots + h_n f_n$ for some $h_i \in \mathbb{k}[x]$ (see Sect. 2.3 on p. 26).

write $E_0 = f_1$, $E_1 = f_2$, and for $k \geq 1$, put

$$E_k = \text{remainder on division of } E_{k-2} \text{ by } E_{k-1}.$$

The degrees of E_k are strictly increasing until the next E_r divides E_{r-1} , and we get $E_{r+1} = 0$. The last nonzero polynomial E_r in the sequence is equal to $\text{GCD}(f_1, f_2)$. During the computation, one can write each E_k as $g_k \cdot E_0 + h_k \cdot E_1$ for some $g_k, h_k \in \mathbb{K}[x]$. Then the output will be represented as $\text{GCD}(f_1, f_2) = E_r = g_r f_1 + h_r f_2$. The next step leads to $E_{r+1} = 0 = g_{r+1} f_1 + h_{r+1} f_2$, where g_{r+1} and $-h_{r+1}$ are coprime associated factors such that $\text{LCM}(f_1, f_2) = g_{r+1} f_1 = -h_{r+1} f_2$.

Exercise 3.8 Prove this.

Example 3.3 Let us carry out the Euclidean algorithm for $f_1(x) = x^7 + 3x^6 + 4x^5 + x^4 + 3x^3 + 5x^2 + 3x + 4$ and $f_2(x) = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4$:

$$E_0 = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4,$$

$$E_1 = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4,$$

$$E_2 = -4x^4 - 13x^3 - 21x^2 - 10x - 8 = E_0 - (x^2 - 2x + 3) E_1;$$

it is more convenient first to divide $16E_1$ by E_2 and then divide the result by 16:

$$\begin{aligned} E_3 &= \frac{1}{16} (x^3 + 5x^2 + 10x + 8) = \frac{1}{16} (16E_1 + (4x + 7) E_2) \\ &= \frac{4x + 7}{16} E_0 - \frac{4x^3 - x^2 - 2x + 5}{16} E_1; \end{aligned}$$

the next step leads to the greatest common divisor:

$$\begin{aligned} E_4 &= -16(x^2 + 3x + 4) = E_2 + 16(4x - 7) E_3 = 16(x^2 - 3) E_0 \\ &\quad - 16(x^4 - 2x^3 + 2x - 2) E_1, \end{aligned}$$

because

$$E_5 = E_3 + (x + 2) \cdot E_4/256 = (x^3 + 2x^2 + x + 1) \cdot E_0 - (x^5 + x^2 + 1) \cdot E_1 = 0.$$

Thus,

$$\begin{aligned} \text{GCD}(f_1, f_2) &= x^2 + 3x + 4 = -(x^2 - 3) f_1(x) + (x^4 - 2x^3 + 2x - 2) f_2(x), \\ \text{LCM}(f_1, f_2) &= (x^3 + 2x^2 + x + 1) f_1(x) = (x^5 + x^2 + 1) f_2(x). \end{aligned}$$

3.3 Roots of Polynomials

Definition 3.4 An element $\alpha \in K$ is called a *root* of the polynomial $f \in K[x]$ if $f(\alpha) = 0$. By Example 3.2 on p. 47, $f(\alpha) = 0$ occurs if and only if $(x - \alpha)$ divides $f(x)$ in $K[x]$.

Exercise 3.9 For a field \mathbb{k} and polynomial $f \in \mathbb{k}[x]$ of degree 2 or 3, show that f is irreducible in $\mathbb{k}[x]$ if and only if f has no roots in \mathbb{k} .

Proposition 3.5 Let K be an integral domain. If a polynomial $f \in K[x]$ has s distinct roots $\alpha_1, \alpha_2, \dots, \alpha_s \in K$, then f is divisible by $\prod_i (x - \alpha_i)$ in $K[x]$. In particular, either $\deg(f) \geq s$ or $f = 0$ in this case.

Proof Write f as $f(x) = (x - \alpha_1) \cdot q(x)$ and substitute $x = \alpha_2, \alpha_3, \dots, \alpha_s$ in this equality. Since $(\alpha_i - \alpha_1) \neq 0$ for all $i \neq 1$ and K has no zero divisors, all the α_i for $i \geq 2$ are roots of $q(x)$. Then we proceed by induction. \square

Corollary 3.2 Every nonzero polynomial f with coefficients in an integral domain K has at most $\deg(f)$ distinct roots in K . \square

Corollary 3.3 Let K be an integral domain and suppose $f, g \in K[x]$ are each of degree at most n . If $f(\alpha_i) = g(\alpha_i)$ for more than n distinct $\alpha_i \in K$, then $f = g$ in $K[x]$.

Proof Since $f - g$ has more than n roots but $\deg(f - g) \leq n$, it must be the zero polynomial. \square

Exercise 3.10 (Lagrange's Interpolating Polynomial) For a field \mathbb{k} , every collection of $n + 1$ distinct points $a_0, a_1, \dots, a_n \in \mathbb{k}$, and arbitrary sequence of values $b_0, b_1, \dots, b_n \in \mathbb{k}$, construct a polynomial $f(x) \in \mathbb{k}[x]$ such that $\deg f \leq n$ and $f(a_i) = b_i$ for all i . Prove that such a polynomial is unique.

3.3.1 Common Roots

Let \mathbb{k} be a field and $K \supset \mathbb{k}$ a commutative ring containing \mathbb{k} as a subring. Polynomials $f_1, f_2, \dots, f_m \in \mathbb{k}[x]$ have a common root $\alpha \in K$ if and only if $x - \alpha$ is a common divisor of all the f_i in $K[x]$. If $h = \text{GCD}(f_1, f_2, \dots, f_m) \in \mathbb{k}[x]$ has positive degree, then every common root of all the f_i is a root of h . Since $\deg h \leq \min \deg f_i$, finding the common roots of a few polynomials often turns out to be easier than doing so for each polynomial individually. In particular, if $\text{GCD}(f_1, f_2, \dots, f_m) = 1$ within $\mathbb{k}[x]$, then f_1, f_2, \dots, f_m have no common roots even in K , because the equality $f_1 h_1 + f_2 h_2 + \dots + f_m h_m = 1$, which holds for some $h_1, h_2, \dots, h_m \in \mathbb{k}[x]$, prohibits the simultaneous vanishing of all the $f_i(a)$ at any point $a \in K$.

3.3.2 Multiple Roots

Let \mathbb{k} be a field as above and $f \in \mathbb{k}[x]$. We say that $\alpha \in \mathbb{k}$ is a root of *multiplicity* m for f if $f(x) = (x - \alpha)^m \cdot g(x)$ in $\mathbb{k}[x]$ and $g(\alpha) \neq 0$. Roots of multiplicity 1 are called *simple*. Roots of multiplicity $m \geq 2$ are called *multiple* or *m-tuple*.

Proposition 3.6 *Let \mathbb{k} be a field, $f \in \mathbb{k}[x]$, and $\alpha \in \mathbb{k}$ a root of f . Then α is a multiple root if and only if $f'(\alpha) = 0$.*

Proof If α is multiple root, then $f(x) = (x - \alpha)^2 g(x)$. Differentiation of both sides leads to $f'(x) = (x - \alpha)(2g(x) + (x - \alpha)g'(x))$ and $f'(\alpha) = 0$. If α is simple, then $f(x) = (x - \alpha)g(x)$, where $g(\alpha) \neq 0$. Now $f'(x) = (x - \alpha)g'(x) + g(x)$ and $f'(\alpha) = g(\alpha) \neq 0$. \square

Proposition 3.7 *Let $\text{char } \mathbb{k} = 0$. A root $\alpha \in \mathbb{k}$ of a polynomial $f \in \mathbb{k}[x]$ has multiplicity $m \geq 2$ if and only if α is an $(m - 1)$ -tuple root of f' . As a consequence, α has multiplicity m if and only if*

$$f(\alpha) = \frac{d}{dx}f(\alpha) = \cdots = \frac{d^{m-1}}{dx^{m-1}}f(\alpha) = 0 \quad \text{but} \quad \frac{d^m}{dx^m}f(\alpha) \neq 0.$$

Proof If $f(x) = (x - \alpha)^m g(x)$, then $f'(x) = (x - \alpha)^{m-1}(mg(x) + (x - \alpha)g'(x))$. For $g(\alpha) \neq 0$ and since $m \neq 0$, the latter factor is not zero for $x = \alpha$. This proves the first statement. The second follows by induction. \square

3.3.3 Separable Polynomials

A polynomial $f \in \mathbb{k}[x]$ is called *separable* if f has no multiple roots in any commutative ring $K \supset \mathbb{k}$. By Proposition 3.6 and what was said in Sect. 3.3.1, a polynomial $f \in \mathbb{k}[x]$ is separable if and only if $\text{GCD}(f, f') = 1$. Note that this condition can be checked by the Euclidean algorithm within $\mathbb{k}[x]$.

Example 3.4 (Irreducible Polynomials) Let $f \in \mathbb{k}[x]$ be irreducible. Then f is coprime to all nonzero polynomials of smaller degree. Therefore, an irreducible polynomial f is separable as soon as $f' \neq 0$. Since for $\text{char } \mathbb{k} = 0$ and $\deg f > 0$ we always have $f' \neq 0$, every irreducible polynomial over a field of characteristic zero is separable. If $\text{char } \mathbb{k} = p > 0$, then $f' = 0$ if and only if $f(x) = g(x^p)$ for some $g \in \mathbb{k}[x]$ as we have seen in Example 3.1 on p. 45. By Lemma 3.1 on p. 45, for $\mathbb{k} = \mathbb{F}_p$ all such polynomials are exhausted by the p th powers g^p , $g \in \mathbb{F}_p[x]$. In particular, they are all reducible. Therefore, all irreducible polynomials in $\mathbb{F}_p[x]$ are separable as well. Over larger fields of characteristic $p > 0$, this may no longer

be true. For example, for the field $\mathbb{k} = \mathbb{F}_p(t)$ of rational functions in the variable⁵ t with coefficients in \mathbb{F}_p , the polynomial $f(x) = x^p - t \in \mathbb{k}[x]$ can be shown to be irreducible.⁶ However, $f' \equiv 0$, i.e., f is not separable.

3.4 Adjunction of Roots

3.4.1 Residue Class Rings

Let \mathbb{k} be a field and $f \in \mathbb{k}[x]$ a nonconstant polynomial. The residue class ring $\mathbb{k}[x]/(f)$ is defined in the same way as the residue class ring $\mathbb{Z}/(n)$ was defined in Sect. 2.4 on p. 27. We write $(f) = \{fh \mid h \in \mathbb{k}[x]\}$ for the subring of all polynomials divisible by f and say that polynomials $g_1, g_2 \in \mathbb{k}[x]$ are *congruent modulo f* if $g_1 - g_2 \in (f)$. In this case, we write $g_1 \equiv g_2 \pmod{f}$.

Exercise 3.11 Verify that congruence modulo f is an equivalence relation on $\mathbb{k}[x]$.

This equivalence decomposes $\mathbb{k}[x]$ into a disjoint union of equivalence classes

$$[g]_f = g + (f) = \{g + fh \mid h \in \mathbb{k}[x]\}$$

called *residue classes modulo f* . Addition and multiplication of residue classes are defined by

$$[g] + [h] \stackrel{\text{def}}{=} [g + h], \quad [g] \cdot [h] \stackrel{\text{def}}{=} [gh]. \quad (3.15)$$

Exercise 3.12 Verify that the classes $[g + h]$ and $[gh]$ do not depend on the particular choice of $g \in [g]$ and $h \in [h]$.

Since the right-hand sides of formulas (3.15) deal with ordinary operations within $\mathbb{k}[x]$, the addition and multiplication of residue classes satisfy the axioms of a commutative ring with unit. The zero element of the ring $\mathbb{k}[x]/(f)$ is $[0]_f = (f)$, and the unit element is $[1]_f = 1 + (f)$. The homomorphism $\mathbb{k} \hookrightarrow \mathbb{k}[x]/(f)$, $c \mapsto [c]_f$, which sends $c \in \mathbb{k}$ to the residue class of the constant polynomial $c \in \mathbb{k}[x]$, is nonzero and therefore injective by Proposition 2.2 on p. 34. In what follows, we identify \mathbb{k} with its image under this embedding and write c instead of $[c]_f$ for $c \in \mathbb{k}$.

Exercise 3.13 Show that $\mathbb{k}[x]/(x - \alpha) \simeq \mathbb{k}$ for all $\alpha \in \mathbb{k}$.

Since every $g \in \mathbb{k}[x]$ is uniquely expressed as $g = fh + r$, where either $\deg r < \deg f$ or $r = 0$, every nonzero residue class $[g]_f$ has a unique representative $r \in [g]_f$

⁵See Sect. 4.2 on p. 76.

⁶With our current equipment it is not so obvious. However, it follows at once from Gauss's lemma (see Lemma 5.4 on p. 117) by means of an Eisenstein-type argument (see Example 5.8 on p. 119).

such that $\deg(r) < \deg(f)$. Therefore, each residue class can be written as

$$[a_0 + a_1x + \cdots + a_{n-1}x^{n-1}] = a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1},$$

where $\vartheta \stackrel{\text{def}}{=} [x]_f$, $a_i \in \mathbb{k}$, and the equality

$$a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1} = b_0 + b_1\vartheta + \cdots + b_{n-1}\vartheta^{n-1}$$

holds in $\mathbb{k}[x]/(f)$ if and only if $a_i = b_i$ in \mathbb{k} for all i .

Note that $\vartheta = [x]_f$ is a root of f , because $f(\vartheta) = f([x]_f) = [f(x)]_f = [0]_f$ in $\mathbb{k}[x]/(f)$. For this reason, the residue class ring $\mathbb{k}[x]/(f)$ is often called an *extension of \mathbb{k} by adjunction of the root ϑ of the polynomial $f \in \mathbb{k}[x]$* . From this viewpoint, addition and multiplication of residue classes can be treated as an ordinary algebraic manipulations with formal expressions

$$a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1} \tag{3.16}$$

obeying the standard rules for multiplying out and collecting like terms except for the one extra relation $f(\vartheta) = 0$ on the symbol ϑ .

For example, the elements of the residue class ring $\mathbb{Q}[x]/(x^2 - 2)$ are represented by formal expressions of the form $a + b\sqrt{2}$, where $\sqrt{2} \stackrel{\text{def}}{=} [x]$ satisfies the relation $(\sqrt{2})^2 = [x]^2 = [x^2] = 2$. Under this relation, the addition and multiplication of such expressions are completely determined by the associative, commutative, and distributive laws:

$$\begin{aligned} (a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2}, \\ (a + b\sqrt{2})(c + d\sqrt{2}) &= (ac + 2bd) + (cb + ad)\sqrt{2}. \end{aligned}$$

Exercise 3.14 Verify that $\mathbb{Q}[x]/(x^2 - 2)$ is a field. Is the same true for residue class rings **(a)** $\mathbb{Q}[x]/(x^3 + 1)$ and **(b)** $\mathbb{Q}[x]/(x^3 + 2)$?

Proposition 3.8 *For a field \mathbb{k} and nonconstant polynomial $f \in \mathbb{k}[x]$, the residue class ring $\mathbb{k}[x]/(f)$ is a field if and only if f is irreducible in $\mathbb{k}[x]$.*

Proof If $f = gh$, where $\deg g, \deg h < \deg f$, then both classes $[g]_f, [h]_f$ are nonzero but have zero product in $\mathbb{k}[x]/(f)$. This prevents the latter from being a field. If f is irreducible, then for every $g \notin (f)$, we have $\text{GCD}(f, g) = 1$, and therefore $fh + gq = 1$ for some $h, q \in \mathbb{k}[x]$. This forces $[q] \cdot [g] = [1]$ in $\mathbb{k}[x]/(f)$. Thus, every nonzero residue class $[g] \in \mathbb{k}[x]/(f)$ is invertible. \square

Exercise 3.15 In $\mathbb{Q}[x]/(x^2 + x + 1)$, write an explicit formula for the inverse element of $\vartheta - a$, where $a \in \mathbb{Q}$ and $\vartheta = [x]$.

Proposition 3.9 (Chinese Remainder Theorem) *Let \mathbb{k} be an arbitrary field and $f \in \mathbb{k}[x]$ a product of m mutually coprime polynomials:*

$$f = f_1 f_2 \cdots f_m, \text{ where } \forall i \neq j, \quad \text{GCD}(f_i, f_j) = 1.$$

Then the isomorphism of commutative rings

$$\varphi : \mathbb{k}[x]/(f) \xrightarrow{\sim} (\mathbb{k}[x]/(f_1)) \times (\mathbb{k}[x]/(f_2)) \times \cdots \times (\mathbb{k}[x]/(f_m))$$

is well defined by $[g]_f \mapsto ([g]_{f_1}, [g]_{f_2}, \dots, [g]_{f_m})$.

Exercise 3.16 Use the arguments from Sect. 2.7 on p. 34 to verify that φ is a well-defined injective ring homomorphism.

Proof (of Proposition 3.9) It remains to verify that φ is surjective, i.e., that for every collection of residue classes $[r_i] \in \mathbb{k}[x]/(f_i)$, there exists a polynomial $g \in \mathbb{k}[x]$ such that $g \equiv r_i \pmod{f_i}$ for all i simultaneously. We proceed as in Example 2.7 on p. 35. For each i , write $F_i = \prod_{v \neq i} f_v$ for the product of all f_v except f_i . Since f_i is coprime to all those f_v , by Lemma 2.3 on p. 26 it is coprime to F_i as well. Hence, there exists some⁷ $h_i \in \mathbb{k}[x]$ such that $F_i h_i \equiv 1 \pmod{f_i}$. Clearly, $F_i h_i \equiv 0 \pmod{f_v}$ for all $v \neq i$. Thus, $\sum_i r_i F_i h_i \equiv r_i \pmod{f_i}$ for all i , as required. \square

3.4.2 Algebraic Elements

Let $\mathbb{k} \subset \mathbb{F}$ be an arbitrary extension of fields. An element $\zeta \in \mathbb{F}$ is said to be *algebraic* over \mathbb{k} if $f(\zeta) = 0$ for some nonzero polynomial $f \in \mathbb{k}[x]$. The monic polynomial of minimal degree with this property is called the *minimal polynomial* of ζ over \mathbb{k} and is denoted by μ_ζ . Every polynomial $f \in \mathbb{k}[x]$ such that $f(\zeta) = 0$ is divisible by μ_ζ , because division with remainder leads to $f(x) = q(x)\mu_\zeta(x) + r(x)$, where either $r = 0$ or $\deg r < \deg \mu_\zeta$, and the latter case is impossible, since $r(\zeta) = f(\zeta) - q(\zeta)\mu_\zeta(\zeta) = 0$. Therefore, the minimal polynomial μ_ζ is uniquely determined by ζ . It is irreducible, because a factorization $\mu_\zeta = g \cdot h$ would force $g(\zeta) = 0$ or $h(\zeta) = 0$, which is impossible for $\deg g, \deg h < \deg \mu$.

For an element $\zeta \in \mathbb{F}$, the evaluation map $\text{ev}_\zeta : \mathbb{k}[x] \rightarrow \mathbb{F}, f \mapsto f(\zeta)$, is a ring homomorphism. Its image $\text{im } \text{ev}_\zeta \subset \mathbb{F}$ is the minimal subring, with respect to inclusion, in \mathbb{F} containing \mathbb{k} and ζ . It is usually denoted by $\mathbb{k}[\zeta]$. If ζ is algebraic over \mathbb{k} , then the above arguments show that $\ker \text{ev}_\zeta = (\mu_\zeta)$ consists of all polynomials divisible by the minimal polynomial of ζ . Hence, the evaluation map can be factorized through the quotient homomorphism $\mathbb{k}[x] \twoheadrightarrow \mathbb{k}[x]/(\mu_\zeta)$ followed by the inclusion of fields $\varphi : \mathbb{k}[x]/(\mu_\zeta) \hookrightarrow \mathbb{F}$ mapping $[f] \mapsto f(\zeta)$. Indeed, φ

⁷This polynomial can be computed explicitly by the Euclidean algorithm applied to F_i and f_i .

is well defined, because $g = f + h\mu_\zeta$ forces $g(\zeta) = f(\zeta)$, and it is injective by Proposition 2.2 on p. 34, because $\mathbb{k}[x]/(\mu_\zeta)$ is a field. We conclude that the smallest subring $\mathbb{k}[\zeta] \subset K$ containing \mathbb{k} and ζ is a field isomorphic to the quotient $\mathbb{k}[x]/(\mu_\zeta)$.

For example, the smallest subring in \mathbb{R} containing \mathbb{Q} and the real number $\sqrt{2} \in \mathbb{R}$ is a field isomorphic to the field $\mathbb{Q}[x]/(x^2 - 2)$ considered before Exercise 3.14 on p. 53.

Theorem 3.1 *For a field \mathbb{k} and polynomial $f \in \mathbb{k}[x]$ of positive degree, there exists a field $\mathbb{F} \supset \mathbb{k}$ such that in $\mathbb{F}[x]$, the polynomial f can be factored completely into a product of $\deg f$ linear factors. Equivalently, f acquires $\deg f$ roots (counted with multiplicities) in \mathbb{F} .*

Proof By induction on $n = \deg f$. For $n = 1$, the statement is trivial. Assume that it holds for all fields \mathbb{k} and all polynomials of degree less than n . Consider a field \mathbb{k} , and let $f \in \mathbb{k}[x]$ have degree n . If $f = gh$, where $\deg g, \deg h < n$, then by induction, there is a field $\mathbb{F}' \supset \mathbb{k}$ such that g is a product of $\deg g$ linear factors in $\mathbb{F}'[x]$. Applying the inductive hypothesis once more to \mathbb{F}' and h , we pass to a field $\mathbb{F} \supset \mathbb{F}'$ over which h is completely factorizable as well. Then $f = gh$ also can be written as a product of $\deg f = \deg g + \deg h$ linear factors in $\mathbb{F}[x]$. If f is irreducible, we put $\mathbb{F}' = \mathbb{k}[x]/(f) \supset \mathbb{k}$. Since f acquires a root $\vartheta = [x] \in \mathbb{F}'$, f becomes divisible by $(x - \vartheta)$ in $\mathbb{F}'[x]$, and we can repeat the previous arguments. \square

3.4.3 Algebraic Closure

A field \mathbb{k} is said to be *algebraically closed* if every polynomial $f \in \mathbb{k}[x]$ has a root in \mathbb{k} . Equivalently, we can say that every $f \in \mathbb{k}[x]$ is completely factorizable into a product of $\deg f$ linear factors (some of which may coincide). One of the most important examples of an algebraically closed field is provided by the field of *complex numbers* \mathbb{C} . We define and study the field \mathbb{C} in the next section. A proof of its algebraic closure⁸ will be sketched in Problem 3.34 on p. 70.

3.5 The Field of Complex Numbers

3.5.1 The Complex Plane

We write $\mathbb{C} \stackrel{\text{def}}{=} \mathbb{R}[t]/(t^2 + 1)$ for the extension of \mathbb{R} by a root of the irreducible quadratic polynomial $t^2 + 1 = 0$. Therefore, \mathbb{C} consists of residue classes $[x + yt] = x + y \cdot i$, where $x, y \in \mathbb{R}$ and $i \stackrel{\text{def}}{=} [t]$ satisfies the relation $i^2 = [t^2] = [-1] = -1$, i.e.,

⁸Although this fact is widely known as the *fundamental theorem of algebra*, its whys and wherefores are rather analytic-geometrical.

it could be written as $i = \sqrt{-1}$. Addition and multiplication in \mathbb{C} are described by the formulas

$$\begin{aligned}(x_1 + iy_1) + (x_2 + iy_2) &= (x_1 + x_2) + i(y_1 + y_2), \\ (x_1 + iy_1)(x_2 + iy_2) &= (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1).\end{aligned}\tag{3.17}$$

The inverse of a nonzero complex number $x + yi \in \mathbb{C}$ is

$$\frac{1}{x + yi} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2} \cdot i.$$

The elements of \mathbb{C} can be depicted in the Euclidean plane \mathbb{R}^2 equipped with a rectangular coordinate system XOY (see Fig. 3.1). A complex number $z = x + yi$ is represented there by a radial vector joining the origin $O = (0, 0)$ to the point $z = (x, y)$. We write $|z| = \sqrt{x^2 + y^2}$ for the length⁹ of this vector. The coordinates x and y are called the *real* and *imaginary parts* of z and are denoted by $\operatorname{Re}(z) = x$ and $\operatorname{Im}(z) = y$. Let

$$\operatorname{Arg}(z) = \alpha + 2\pi\mathbb{Z} = \{\alpha + 2\pi k \in \mathbb{R} \mid k \in \mathbb{Z}\}\tag{3.18}$$

be the set of all $\vartheta \in \mathbb{R}$ such that a rotation of the plane about the origin through the angle ϑ (measured in radians) moves the ray OX to the ray Oz . All these angles are congruent modulo integer multiples of 2π and are equal to oriented¹⁰ lengths of arc of the unit circle S^1 going from $(1, 0)$ to the intersection point of S^1 with the ray Oz . We write $\alpha \in \operatorname{Arg}(z)$ for the oriented length of the shortest among such arcs. The congruence class (3.18) is called the *argument* of z . Thus, each $z = x + yi \in \mathbb{C}$ has $\operatorname{Re}(z) = |z| \cdot \cos \alpha$, $\operatorname{Im}(z) = |z| \cdot \sin \alpha$, and can be written as $z = |z| \cdot (\cos \alpha + i \cdot \sin \alpha)$.

Lemma 3.2 *The radial vectors of the points $z \in \mathbb{R}^2$ form a field with respect to the usual addition of vectors¹¹ and multiplication defined by the rule that lengths are multiplied, arguments are added, i.e., by the formulas*

$$\begin{aligned}|z_1 z_2| &\stackrel{\text{def}}{=} |z_1| \cdot |z_2|, \\ \operatorname{Arg}(z_1 z_2) &\stackrel{\text{def}}{=} \operatorname{Arg}(z_1) + \operatorname{Arg}(z_2) = \{\vartheta_1 + \vartheta_2 \mid \vartheta_1 \in \operatorname{Arg}(z_1), \vartheta_2 \in \operatorname{Arg}(z_2)\}.\end{aligned}\tag{3.19}$$

This field is isomorphic to \mathbb{C} . The isomorphism takes the complex number $x + iy \in \mathbb{C}$ to the radial vector of the point $z = (x, y) \in \mathbb{R}^2$.

⁹Also called the *modulus* or *absolute value* of z .

¹⁰That is, taken with a positive sign when an arc goes counterclockwise and with a negative sign otherwise.

¹¹See Example 2.4 on p. 22.

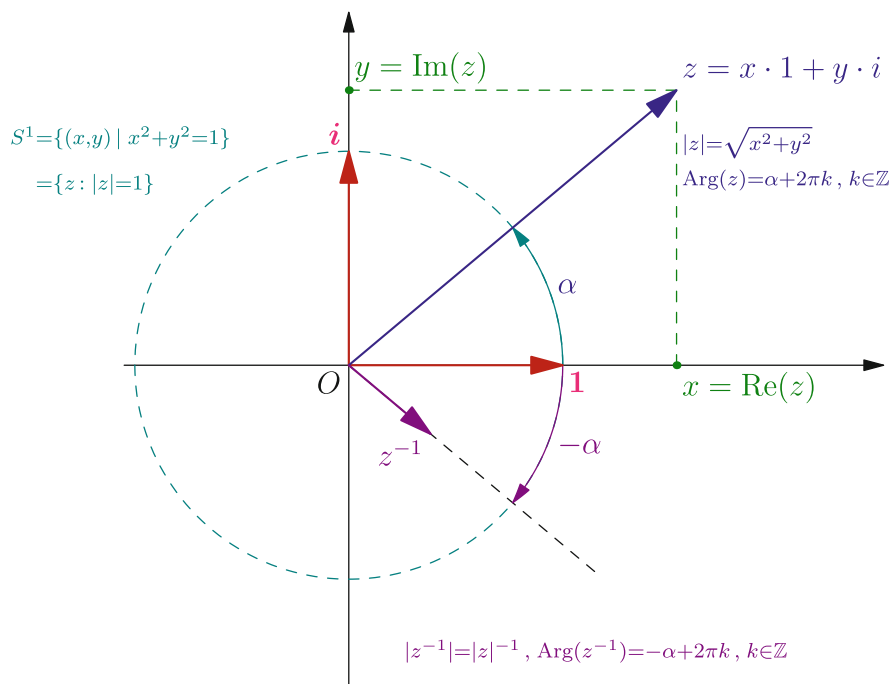


Fig. 3.1 Geometric ingredients of a complex number

Exercise 3.17 Check that the addition of arguments used in the second formula of (3.19) is well defined in the sense that the right-hand side is actually a congruence class modulo $2\pi \cdot \mathbb{Z}$, as it must be by formula (3.18).

Proof (of Lemma 3.2) We have seen in Example 2.4 on p. 22 that vectors form an additive abelian group. Multiplication (3.19) is clearly commutative and associative. The unit direction vector of the OX -axis, which has length 1 and argument 0, is the neutral element for multiplication. The inverse of a nonzero vector z is the vector z^{-1} , which has $|z^{-1}| = 1/|z|$ and $\operatorname{Arg}(z^{-1}) = -\operatorname{Arg}(z)$ (see Fig. 3.1). Therefore, the nonzero vectors form a multiplicative abelian group whose unit element differs from zero. It remains to check distributivity. The multiplication map $\lambda_a : z \mapsto az$, which multiplies all vectors by some fixed vector $a \neq 0$, is a rotary dilation¹² of \mathbb{R}^2 at the origin by the angle $\operatorname{Arg}(a)$ and scaling factor $|a|$. The distributive law $a(b + c) = ab + ac$ says that a rotary dilation respects the addition of vectors, i.e., $\lambda_a(b + c) = \lambda_a(b) + \lambda_a(c)$. This is true, because both rotations and dilations take parallelograms to parallelograms. Hence, the radial vectors of points in \mathbb{R}^2

¹²That is, the composition of a rotation and dilation with the same center (since they commute, it does not matter which one was done first).

form a field. It contains a subfield formed by the vectors parallel to the OX -axis. Let us identify this subfield with¹³ \mathbb{R} and write i for the unit direction vector of the OY -axis. The radial vector of a point $z = (x, y) \in \mathbb{R}^2$ can be uniquely expressed as $z = x + i \cdot y$, where $x, y \in \mathbb{R}$ (i.e., they are parallel to the OX -axis), and the operations $+$, \cdot are those from formula (3.19). It follows from (3.19) that $i^2 = -1$. Thus, by distributivity, the addition and multiplication of vectors $x_1 + iy_1$ and $x_2 + iy_2$ are described by the same rules (3.17) as the addition and multiplication in the quotient field $\mathbb{C} = \mathbb{R}[t]/(t^2 + 1)$. \square

Agreement 3.1 From this point on, we shall identify the field $\mathbb{C} = \mathbb{R}[t]/(t^2 + 1)$ with the field of radial vectors in \mathbb{R}^2 . We shall refer to the *complex plane* when we switch to a geometric interpretation of the complex numbers. The coordinate axes OX and OY are called the *real* and *imaginary* axes of the complex plane.

3.5.2 Complex Conjugation

The complex number $\bar{z} \stackrel{\text{def}}{=} x - iy$ is called the *conjugate* of the complex number $z = x + iy$. Since $z\bar{z} = x^2 + y^2 = |z|^2$, we get the very convenient inversion formula $z^{-1} = \bar{z}/|z|^2$. Geometrically, the conjugation map $\mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto \bar{z}$, is the reflection of the complex plane in the real axis. Algebraically, complex conjugation is an involutive¹⁴ automorphism of the field \mathbb{C} over the subfield $\mathbb{R} \subset \mathbb{C}$. This means that $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$ and $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$ for all $z_1, z_2 \in \mathbb{C}$, $\bar{\bar{z}} = z$ for all $z \in \mathbb{C}$, and $z = \bar{z}$ if and only if $z \in \mathbb{R}$.

3.5.3 Trigonometry

You probably studied trigonometry in high school and perhaps even recall some of that depressing conglomeration of trigonometric identities. If so, your long nightmare is over. Those trigonometric identities are just simple polynomial expressions in $z \in \mathbb{C}$ restricted to the unit circle $S^1 \subset \mathbb{R}$ and rewritten in terms of the real and imaginary parts x, y now given the names $\cos \varphi$ and $\sin \varphi$. In most cases, this separation into sine and cosine has the effect of making a simple expression more complicated.

For example, consider two complex numbers $z_1 = \cos \varphi_1 + i \sin \varphi_1$, $z_2 = \cos \varphi_2 + i \sin \varphi_2$ on the unit circle, where $\varphi_1 \in \text{Arg}(z_1)$, $\varphi_2 \in \text{Arg}(z_2)$. Then their product, computed by (3.19), is $z_1 z_2 = \cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)$, whereas the

¹³Note that the multiplication in \mathbb{R} agrees with that defined in (3.19).

¹⁴An endomorphism $\iota : X \rightarrow X$ of a set X is called an *involution* if $\iota \circ \iota = \text{Id}_X$.

formula (3.17) leads to

$$z_1 z_2 = (\cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2) + i(\cos \varphi_1 \sin \varphi_2 + \sin \varphi_1 \cos \varphi_2).$$

Comparison of the real and imaginary parts proves at once the two most famous trigonometric formulas:

$$\cos(\varphi_1 + \varphi_2) = \cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2$$

$$\sin(\varphi_1 + \varphi_2) = \cos \varphi_1 \sin \varphi_2 + \sin \varphi_1 \cos \varphi_2.$$

Example 3.5 (Multiple Angles) Let us take $z = \cos \varphi + i \sin \varphi$ and compute $z^n = \cos(n\varphi) + i \sin(n\varphi)$ by expanding $(\cos \varphi + i \sin \varphi)^n$ via the binomial formula (1.7) on p. 6. We get

$$\begin{aligned} \cos(n\varphi) + i \sin(n\varphi) &= (\cos \varphi + i \sin \varphi)^n \\ &= \cos^n \varphi + i \binom{n}{1} \cos^{n-1} \varphi \sin \varphi - \binom{n}{2} \cos^{n-2} \varphi \sin^2 \varphi - i \binom{n}{3} \cos^{n-3} \varphi \sin^3 \varphi \\ &\quad + \dots \\ &= \left(\binom{n}{0} \cos^n \varphi - \binom{n}{2} \cos^{n-2} \varphi \sin^2 \varphi + \binom{n}{4} \cos^{n-4} \varphi \sin^4 \varphi - \dots \right) \\ &\quad + i \cdot \left(\binom{n}{1} \cos^{n-1} \varphi \sin \varphi - \binom{n}{3} \cos^{n-3} \varphi \sin^3 \varphi + \binom{n}{5} \cos^{n-5} \varphi \sin^5 \varphi \right. \\ &\quad \left. - \dots \right). \end{aligned}$$

This equality describes the entire trigonometry of multiple angles:

$$\begin{aligned} \cos(n\varphi) &= \binom{n}{0} \cos^n \varphi - \binom{n}{2} \cos^{n-2} \varphi \sin^2 \varphi + \binom{n}{4} \cos^{n-4} \varphi \sin^4 \varphi - \dots, \\ \sin(n\varphi) &= \binom{n}{1} \cos^{n-1} \varphi \sin \varphi - \binom{n}{3} \cos^{n-3} \varphi \sin^3 \varphi + \binom{n}{5} \cos^{n-5} \varphi \sin^5 \varphi \\ &\quad - \dots. \end{aligned}$$

For example, $\cos 3\varphi = \cos^3 \varphi - 3 \cos \varphi \cdot \sin^2 \varphi = 4 \cos^3 \varphi - 3 \cos^2 \varphi$.

Exercise 3.18 Express $\sin(2\pi/5)$ and $\cos(2\pi/5)$ in terms of roots of rational numbers.

3.5.4 Roots of Unity and Cyclotomic Polynomials

Let us solve the equation $z^n = 1$ in \mathbb{C} . Comparison of absolute values leads to $|z^n| = |z|^n = 1$ and forces $|z| = 1$. Comparison of arguments gives $n\text{Arg}(z) = \text{Arg}(1) = \{2\pi k \mid k \in \mathbb{Z}\}$, meaning that $\text{Arg}(z) = \{2\pi k/n \mid k \in \mathbb{Z}\}$. Therefore, the polynomial $z^n - 1$ has exactly n distinct complex roots

$$\zeta_k = \cos(2\pi k/n) + i \sin(2\pi k/n), \text{ where } k = 0, 1, \dots, (n-1).$$

They form the vertices of a regular n -gon inscribed in the unit circle in such a way that $\zeta_0 = 1$ (see Fig. 3.2 on p. 60). These roots form a multiplicative abelian group called the group of n th roots of unity and denoted by μ_n . The group μ_n is isomorphic to the cyclic group of order n from Example 1.8 on p. 13.

A root $\zeta \in \mu_n$ is called *primitive*¹⁵ if its powers $\zeta^k, k \in \mathbb{N}$, exhaust the whole of μ_n . For example, the root of minimal positive argument

$$\zeta_1 = \cos(2\pi/n) + i \sin(2\pi/n)$$

is always primitive. All four nontrivial roots of μ_5 are primitive (see Fig. 3.2). In μ_6 , there are just two primitive roots, ζ_1 and $\zeta_5 = \zeta_1^{-1}$ (see Fig. 3.3 on p. 61).

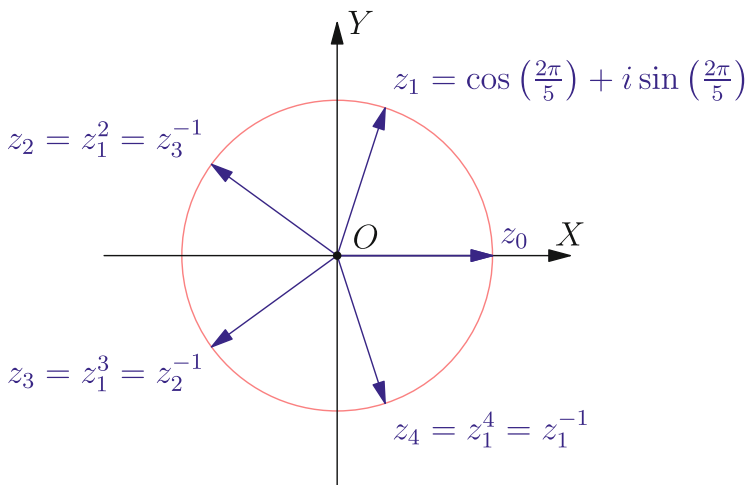


Fig. 3.2 Roots of $z^5 = 1$

Exercise 3.19 Verify that the root $\zeta_1^k = \cos(2\pi k/n) + i \sin(2\pi k/n)$ is primitive in μ_n if and only if $\text{GCD}(k, n) = 1$.

¹⁵In other terminology, a *generating root* of unity.

The monic polynomial whose roots are exactly the primitive n th roots of unity is denoted by

$$\Phi_n(z) = \prod_{\substack{1 \leq k < n : \\ \text{GCD}(k,n)=1}} (z - z_1^k) \quad (3.20)$$

and called the n th cyclotomic polynomial. For example, the fifth and sixth cyclotomic polynomials are

$$\Phi_5(z) = (z - z_1)(z - z_2)(z - z_3)(z - z_4) = z^4 + z^3 + z^2 + z + 1,$$

$$\Phi_6(z) = (z - z_1)(z - z_4) = z^2 - z + 1.$$

One can show¹⁶ that all cyclotomic polynomials are irreducible and have integer coefficients. Some basic properties of Φ_n are listed in [Problem 3.32](#) on p. 70 below.

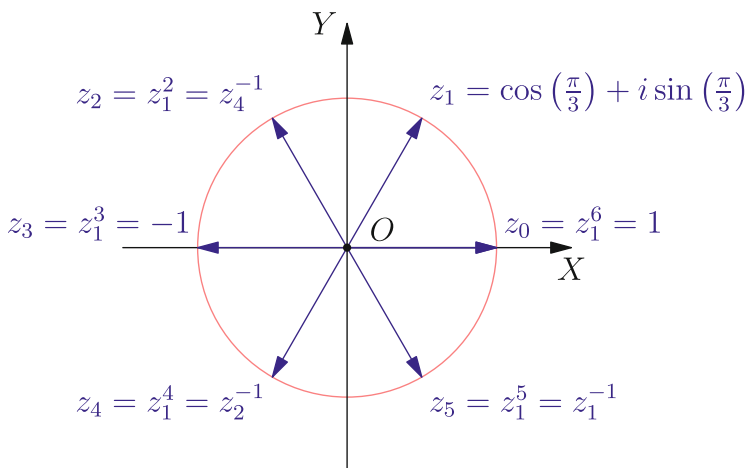


Fig. 3.3 Roots of $z^6 = 1$

Example 3.6 (The Equation $z^n = a$) The complex roots of the equation $z^n = a$, where $a = |a| \cdot (\cos \alpha + i \sin \alpha) \neq 0$, are the numbers

$$z_k = \sqrt[n]{|a|} \cdot \left(\cos \frac{\alpha + 2\pi k}{n} + i \cdot \sin \frac{\alpha + 2\pi k}{n} \right), \quad 0 \leq k \leq n-1.$$

¹⁶This is not so easy, and we shall return to this problem in the forthcoming Algebra II.

They form the vertices of a regular n -gon inscribed in a circle of radius $\sqrt[n]{|a|}$ centered at the origin and rotated in such a way that the radial vector of one of vertices forms the angle α/n with the OX -axis.

3.5.5 The Gaussian Integers

The complex numbers with integer coordinates form a subring in \mathbb{C} denoted by $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{z = x + iy \mid x, y \in \mathbb{Z}\}$ and called the ring of *Gaussian integers*. The Gaussian integers are widely used in number theory. For example, they clarify the following classical problem: which integers $m \in \mathbb{Z}$ can be written in the form $x^2 + y^2$ for some $x, y \in \mathbb{Z}$? Since $x^2 + y^2 = (x + iy)(x - iy)$ in $\mathbb{Z}[i]$, the solvability of the equation $m = x^2 + y^2$ in $x, y \in \mathbb{Z}$ is equivalent to the solvability of the equation $m = z \cdot \bar{z}$ in $z \in \mathbb{Z}[i]$. If the latter is solvable for some $m_1, m_2 \in \mathbb{Z}$, i.e.,

$$m_1 = a_1^2 + b_1^2 = (a_1 + ib_1)(a_1 - ib_1) = z_1 \bar{z}_1,$$

$$m_2 = a_2^2 + b_2^2 = (a_2 + ib_2)(a_2 - ib_2) = z_2 \bar{z}_2,$$

then it is solvable for the product $m = m_1 m_2$ as well:

$$m = z_1 z_2 \cdot \overline{z_1 z_2} = |z_1 z_2|^2 = (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_2 b_1)^2.$$

This reduces the question to the representability of prime numbers. We postpone further analysis until Example 5.6 on p. 115.

Exercise 3.20 Show that $\mathbb{Z}[i]$ has exactly four invertible elements: ± 1 and $\pm i$.

3.6 Finite Fields

3.6.1 Finite Multiplicative Subgroups in Fields

In this section we consider abelian groups with a multiplicative group operation. Such a group A is called *cyclic* if there exists an element $a \in A$ whose integer powers a^n , $n \in \mathbb{Z}$, exhaust the whole group. An element $a \in A$ possessing this property is called a *generator* of the cyclic group A . For example, the group of n th roots of unity $\mu_n \subset \mathbb{C}$ is cyclic, and its generators are the primitive roots.¹⁷

If A is a finite group, then the integer powers of an element $b \in A$ cannot all be distinct, i.e., $b^k = b^m$ for some $k > m$. This forces $b^{k-m} = 1$. The minimal $m \in \mathbb{N}$ such that $b^m = 1$ is called the *order* of b and is denoted by $\text{ord}(b)$. If $\text{ord}(b) = n$, then the n elements $b^0 \stackrel{\text{def}}{=} 1, b^1 = b, b^2, \dots, b^{n-1}$ are distinct and exhaust the set of

¹⁷See Sect. 3.5.4 on p. 60.

all integer powers b^m , because $b^{nq+r} = (b^n)^q b^r = b^r$ for every $m = nq + r \in \mathbb{Z}$. Note that b generates A if and only if $\text{ord}(b) = |A|$; thus the cardinality of the cyclic group coincides with the order of every generator of the group.

Theorem 3.2 *Every finite subgroup A of the multiplicative group \mathbb{k}^* of a field \mathbb{k} is cyclic.*

Proof Let $m = \max_{b \in A} \text{ord}(b)$. If the order of every element in A divides m , then all of them are roots of the polynomial $x^m - 1 = 0$. Since this polynomial has at most m roots in the field \mathbb{k} by Corollary 3.2 on p. 50, we get the inequality $|A| \leq m$, which forces every element of order m to be a generator of A . To prove that the orders of all elements in A divide the maximal order, it is sufficient to construct an element $b \in A$ of order $\text{LCM}(m_1, m_2)$ for any two elements $b_1, b_2 \in A$ of distinct orders m_1, m_2 .

Exercise 3.21 Use Exercise 2.8 to find coprime $n_1, n_2 \in \mathbb{N}$ such that $m_1 = k_1 n_1$, $m_2 = k_2 n_2$, $\text{GCD}(k_1, n_1) = \text{GCD}(k_2, n_2) = 1$, and $\text{LCM}(m_1, m_2) = n_1 n_2$.

Let $a_1 = b_1^{k_1}$, $a_2 = b_2^{k_2}$, where k_1, k_2 are from Exercise 3.21. Then $\text{ord}(a_1) = n_1$ and $\text{ord}(a_2) = n_2$ are coprime. Let us check that $\text{ord}(a_1 a_2) = n_1 n_2$, as required. If $(a_1 a_2)^c = 1$, then $a_1^c = a_2^{n_2 - c}$ and $a_2^{n_1(n_2 - c)} = a_1^{n_1 c} = 1$. Therefore, $n_1(n_2 - c) : n_2$. Hence, $c : n_2$. By symmetry, $c : n_1$ as well. Since n_1 and n_2 are coprime, $c : n_1 n_2$. \square

3.6.2 Description of All Finite Fields

For an irreducible polynomial $f \in \mathbb{F}_p[t]$ of degree n , the residue field $\mathbb{F}_p[t]/(f)$ consists of p^n elements of the form $a_0 + a_1 \vartheta + \cdots + a_{n-1} \vartheta^{n-1}$, where $a_i \in \mathbb{F}_p$ and $f(\vartheta) = 0$.

For example, the polynomial $t^2 + 1 \in \mathbb{F}_3[t]$ is irreducible, because it has no roots in \mathbb{F}_3 . Therefore, the residue ring $\mathbb{F}_9 \stackrel{\text{def}}{=} \mathbb{F}_3/(t^2 + 1)$ is a field of nine elements $a + bi$, where $a, b \in \mathbb{F}_3 = \{-1, 0, 1\}$ and $i \stackrel{\text{def}}{=} [t]$ satisfies $i^2 = -1$. The field extension $\mathbb{F}_3 \subset \mathbb{F}_9$ is analogous to the extension $\mathbb{R} \subset \mathbb{C}$. For example, the Frobenius automorphism $F_3 : \mathbb{F}_9 \rightarrow \mathbb{F}_9$, $a \mapsto a^3$, takes $a + bi$ to $a - bi$ and looks like complex conjugation.

Similarly, the polynomial $t^2 + t + 1 \in \mathbb{F}_2[t]$ is irreducible, because it has no roots in \mathbb{F}_2 . The field $\mathbb{F}_4 \stackrel{\text{def}}{=} \mathbb{F}_2[t]/(t^2 + t + 1)$ consists of four elements¹⁸: $0, 1, \omega \stackrel{\text{def}}{=} [t]$, and $1 + \omega = \omega^2 = \omega^{-1}$. The extension $\mathbb{F}_2 \subset \mathbb{F}_4$ also becomes analogous to the extension $\mathbb{R} \subset \mathbb{C}$ as soon we represent the field \mathbb{C} as the extension of \mathbb{R} by a root of the cyclotomic trinomial $\Phi_3(t) = t^2 + t + 1$, i.e., as¹⁹

$$\mathbb{C} = \mathbb{R}[t]/(t^2 + t + 1) = \{u + w\omega \mid u, w \in \mathbb{R}, \omega = (-1 + i\sqrt{3})/2 \in \mathbb{C}\}.$$

¹⁸Note that the equality $-1 = 1$ in \mathbb{F}_2 allows us to avoid the minus sign.

¹⁹The standard Cartesian coordinates (x, y) in \mathbb{C} are related to the “triangular coordinates” (u, w) of the same point $x + iy = z = u + w\omega$ by $x = u - w/2$, $y = \sqrt{3}w/2$.

Again, the Frobenius automorphism $F_2 : \mathbb{F}_4 \rightarrow \mathbb{F}_4, a \mapsto a^2$, maps $\omega \mapsto \bar{\omega} = \omega^2$ and is similar to complex conjugation: both act identically on the subfields being extended and swap the roots of the trinomial $t^2 + t + 1$.

Exercise 3.22 Write down the multiplication tables and the tables of inverse elements for the fields \mathbb{F}_4 and \mathbb{F}_9 . List all squares, all cubes, and all generators of the multiplicative groups \mathbb{F}_4^* and \mathbb{F}_9^* .

Lemma 3.3 *For finite fields $\mathbb{k} \subset \mathbb{F}$, there exists $n \in \mathbb{N}$ such that $|\mathbb{F}| = |\mathbb{k}|^n$.*

Proof We use induction²⁰ on the difference $|\mathbb{F}| - |\mathbb{k}|$. The case $|\mathbb{F}| = |\mathbb{k}|$ is trivial. If there exists $\zeta \in \mathbb{F} \setminus \mathbb{k}$, then ζ is algebraic over \mathbb{k} , because $\zeta^k = \zeta^\ell$ for some $k \neq \ell$ in the finite field \mathbb{F} . We know from Sect. 3.4.2 on p. 54 that there is a subfield $\mathbb{k}[\zeta] \subset \mathbb{F}$ isomorphic to $\mathbb{k}[x]/(\mu_\zeta)$, where $\mu_\zeta \in \mathbb{k}[x]$ is the minimal polynomial of ζ over \mathbb{k} . Let $\deg \mu_\zeta = m$. Then $\mathbb{k}[\zeta]$ consists of $|\mathbb{k}|^m$ elements $a_0 + a_1\zeta + \cdots + a_{m-1}\zeta^{m-1}$, $a_i \in \mathbb{k}$. By the inductive hypothesis applied to the extension $\mathbb{k}[\zeta] \subset \mathbb{F}$, there exists $n \in \mathbb{N}$ such that $|\mathbb{F}| = |\mathbb{k}[\zeta]|^n = |\mathbb{k}|^{mn}$. \square

Corollary 3.4 *The cardinality of a finite field is equal to a power of its characteristic.* \square

Theorem 3.3 *For every $n \in \mathbb{N}$ and prime $p \in \mathbb{N}$, there exists a finite field \mathbb{F}_q of characteristic p and cardinality $q = p^n$.*

Proof Consider the polynomial $f(x) = x^q - x \in \mathbb{F}_p[x]$. By Theorem 3.1, there exists a field $\mathbb{F} \supset \mathbb{F}_p$ such that f acquires n roots in \mathbb{F} . Since $f' \equiv 1$, all these roots are distinct. In other words, there are exactly q distinct elements $\alpha \in \mathbb{F}$ such that $\alpha^q = \alpha$. They form a field, because $\alpha^q = \alpha$ implies $(-\alpha)^q = -\alpha$ and $(\alpha^{-1})^q = \alpha^{-1}$, and if $\beta = \beta^q$, then $\alpha\beta = \alpha^q\beta^q = (\alpha\beta)^q$ and $\alpha + \beta = \alpha^{p^n} + \beta^{p^n} = F_p^n(\alpha) + F_p^n(\beta) = F_p^n(\alpha + \beta) = (\alpha + \beta)^{p^n}$, where $F_p : \mathbb{F} \rightarrow \mathbb{F}, x \mapsto x^p$, is the Frobenius endomorphism. \square

Theorem 3.4 *Two finite fields are isomorphic if and only if they have equal cardinalities.*

Proof Let \mathbb{F} be a field with $|\mathbb{F}| = q$ and $\text{char } \mathbb{F} = p$. Then $q = p^n$ by Corollary 3.4. It is enough to show that \mathbb{F} is isomorphic to the field \mathbb{F}_q constructed in the proof of Theorem 3.3. The multiplicative group \mathbb{F}^* is cyclic by Theorem 3.2 on p. 63. Choose some generator ζ of \mathbb{F}^* and write $\mu_\zeta \in \mathbb{F}_p[x]$ for the minimal polynomial of ζ over \mathbb{F}_p . Thus, $\mathbb{F} = \mathbb{F}_p[\zeta]$ is isomorphic to $\mathbb{F}_p[x]/(\mu_\zeta)$, as we have seen in Sect. 3.4.2 on p. 54. Since the polynomial $f(x) = x^q - x$ vanishes at ζ , it is divisible by μ_ζ in $\mathbb{F}_p[x]$, i.e., $f = \mu_\zeta g$, where $\deg g < \deg f$. Since f has q distinct roots in \mathbb{F}_q , the polynomial μ_ζ should have at least one root ξ in \mathbb{F}_q , since otherwise, g would have too many roots. As soon as $\mu_\zeta(\xi) = 0$, the assignment $[h] \mapsto h(\xi)$ gives a

²⁰We take such a roundabout way because the vector-space machinery will not appear until Chap. 6. Indeed, \mathbb{F} is a finite-dimensional vector space over $\mathbb{k} \subset \mathbb{F}$, and Lemma 3.3 follows at once from Corollary 6.3 on p. 133.

well-defined homomorphism $\mathbb{F}_p[x]/(\mu_\zeta) \hookrightarrow \mathbb{F}_q$. It maps $[1] \mapsto 1$ and therefore is injective by Proposition 2.2 on p. 34. Since both fields consist of q elements, it is surjective as well. Thus, the fields \mathbb{F} , \mathbb{F}_q are isomorphic to the same residue field $\mathbb{F}_p[x]/(\mu_\zeta)$. \square

3.6.3 Quadratic Residues

Fix a prime integer $p > 2$. The squares in the multiplicative group \mathbb{F}_p^* are called *quadratic residues* modulo p . All the other elements in \mathbb{F}_p^* are called *quadratic nonresidues* or just *nonresidues* for short. The quadratic residues form a multiplicative subgroup in \mathbb{F}_p^* , the image of the multiplicative group homomorphism $\mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$, $x \mapsto x^2$. The kernel of this homomorphism consists of two elements, because $x^2 = 1$ exactly for $x = \pm 1$ in the field \mathbb{F}_p . We conclude that there are precisely $(p-1)/2$ quadratic residues in \mathbb{F}_p^* .

Fermat's little theorem²¹ allows us to check whether a given residue $a \in \mathbb{F}_p^*$ is quadratic. Namely, since $a^{p-1} = 1$ for all $a \in \mathbb{F}_p^*$, the image of another homomorphism of multiplicative groups,

$$\mathbb{F}_p^* \rightarrow \mathbb{F}_p^*, \quad x \mapsto x^{(p-1)/2}, \quad (3.21)$$

lies inside the roots of the polynomial $x^2 - 1$. The equation $x^{(p-1)/2} = 1$ has at most $(p-1)/2 < p-1$ roots in \mathbb{F}_p . Thus, the homomorphism (3.21) maps \mathbb{F}_p^* onto $\{\pm 1\}$ surjectively. Therefore, its kernel consists of $(p-1)/2$ elements. Since all quadratic residues lie in the kernel, we conclude that $a \in \mathbb{F}_p^*$ is a quadratic residue if and only if $a^{(p-1)/2} = 1$. For example, -1 is a square in \mathbb{F}_p if and only if $(p-1)/2$ is even.

For $n \in \mathbb{N}$ and prime $p > 2$, write $[n]_p \in \mathbb{F}_p$ for the residue class of n . The quantity

$$\left(\frac{n}{p}\right) \stackrel{\text{def}}{=} [n]_p^{(p-1)/2} = \begin{cases} 1, & \text{if } [n]_p \in \mathbb{F}_p^* \text{ is a quadratic residue,} \\ 0, & \text{if } [n]_p = 0, \\ -1, & \text{if } [n]_p \in \mathbb{F}_p^* \text{ is a quadratic nonresidue,} \end{cases} \quad (3.22)$$

is called the *Legendre–Jacobi symbol* of n modulo the prime p . It depends only on $n \pmod{p}$ and is multiplicative in n in the sense that

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right).$$

²¹See Theorem 2.1 on p. 30.

Exercise 3.23*. Prove that for every prime $p > 2$, one has $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{8}$.

The Legendre–Jacobi symbol can be computed easily thanks to the following *quadratic reciprocity law*, discovered by Euler and first proved by Gauss:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \quad \text{for all prime integers } p, q > 2. \quad (3.23)$$

Two proofs of this theorem found by Eisenstein and Zolotarev are sketched in [Problem 3.38](#) on p. 71 and in [Problem 9.7](#) on p. 225. Here is an example of how it works:

$$\left(\frac{57}{179}\right) = \left(\frac{179}{57}\right) = \left(\frac{8}{57}\right) = \left(\frac{2}{57}\right)^3 = 1.$$

Thus, 57 is a square modulo 179.

Problems for Independent Solution to Chap. 3

Problem 3.1 Show that $x^m - 1$ divides $x^n - 1$ for $n \mid m$.

Problem 3.2 In the ring $\mathbb{Z}[x]$, find the residues on division of $x^{179} + x^{57} + x^2 + 1$ by
(a) $x^2 - 1$, (b) $x^2 + 1$, (c) $x^2 + x + 1$.

Problem 3.3 Find all multiple complex roots of the polynomial

$$x^7 + 7x^5 - 36x^4 + 15x^3 - 216x^2 + 9x - 324.$$

Problem 3.4 Check whether $\mathbb{R}[x]/(f)$ is a field for (a) $f = x^4 + 1$, (b) $f = x^3 + 1$,
(c) $f = x^2 + 3$.

Problem 3.5 Given $\vartheta \in \mathbb{C}$, write $\mathbb{Q}[\vartheta] \subset \mathbb{C}$ for the smallest subfield containing ϑ .
Are there any isomorphic fields among $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, and $\mathbb{Q}[\sqrt[3]{2}]$?

Problem 3.6 Find the minimal polynomial²² of (a) $2 - 3i \in \mathbb{C}$ over \mathbb{R} , (b) $\sqrt{2} + \sqrt{3} \in \mathbb{R}$ over \mathbb{Q} .

Problem 3.7 For the finite field \mathbb{F}_q , show that every function $\mathbb{F}_q \rightarrow \mathbb{F}_q$ can be written as $a \mapsto f(a)$ for an appropriate $f \in \mathbb{F}_q[x]$ and give an example of two different polynomials producing the same functions $\mathbb{F}_q \rightarrow \mathbb{F}_q$.

²²See Sect. 3.4.2 on p. 54.

Problem 3.8 Find a monic polynomial of the lowest possible degree with coefficients in $\mathbb{Z}/(n)$ that produces the zero function $\mathbb{Z}/(n) \rightarrow \mathbb{Z}/(n)$ for (a) $n = 101$, (b) $n = 111$, (c) $n = 121$.

Problem 3.9 Show that for every field²³ \mathbb{k} , the polynomial ring $\mathbb{k}[x]$ contains

- (a) infinitely many irreducible polynomials,
- (b) an irreducible polynomial of every degree.

Problem 3.10 List all irreducible polynomials of degree ≤ 5 in $\mathbb{F}_2[x]$ and all irreducible polynomials of degree ≤ 3 in $\mathbb{F}_3[x]$.

Problem 3.11 How many irreducible polynomials of degrees 3 and 4 are there in $\mathbb{F}_3[x]$?

Problem 3.12 Use an appropriate modification of Möbius inversion²⁴ to prove that $\mathbb{F}_p[x]$ has exactly $\frac{1}{n} \sum_{d|n} p^d \mu(n/d)$ irreducible polynomials of degree n .

Problem 3.13 Write \mathbb{F}_q for a finite field of $q = p^n$ elements and $\mathbb{F}_p \subset \mathbb{F}_q$ for its prime subfield. Show that the order of every element in the multiplicative group \mathbb{F}_q^* divides $q - 1$. Use Problem 3.1 to show that for each $d \mid n$, there are exactly d distinct elements $x \in \mathbb{F}_q^*$ satisfying the equation $x^d = 1$. Then use an appropriate modification of the Möbius inversion formula²⁵ to compute the number of elements of order d in \mathbb{F}_q^* . In particular, find the total number of elements of order $(q - 1)$ and deduce from this²⁶ that the multiplicative group \mathbb{F}_q^* is cyclic. What can the degree of the minimal polynomial for an element of order $(q - 1)$ in \mathbb{F}_q^* be?

Problem 3.14 Show that for a field \mathbb{k} of characteristic $p > 0$ and $a \in \mathbb{k}$, the polynomial $x^p - a$ either is irreducible in $\mathbb{k}[x]$ or has a root of multiplicity p in \mathbb{k} .

Problem 3.15 Let the polynomial $f(x) = x^p - x - a \in \mathbb{F}_p[x]$ have a root ζ in some field $\mathbb{F} \supset \mathbb{F}_p$. Find another $p - 1$ roots of f in \mathbb{F} and prove that in $\mathbb{F}_p[x]$, the polynomial f is either irreducible or completely factorizable as a product of linear binomials.

Problem 3.16 Show that every polynomial $f \in \mathbb{R}[x]$ is a product of linear binomials and quadratic trinomials with negative discriminants. Write such a factorization for $f = x^8 + 128$.

Problem 3.17 (Viète's Formulas) Given a monic polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

express its coefficients a_k in terms of the roots α_v and determine a constant $\vartheta = \vartheta(a_1, a_2, \dots, a_n)$ such that $f(t - \vartheta)$ has no term of degree $n - 1$.

²³Especially for a finite one.

²⁴See Problem 2.20 on p. 39.

²⁵See Problem 2.20 on p. 39.

²⁶Independently of Theorem 3.2 on p. 63.

Problem 3.18 (Discriminant) In the notation of [Problem 3.17](#), the quantity

$$D_f \stackrel{\text{def}}{=} \prod_{i < j} (\alpha_i - \alpha_j)^2$$

is called the *discriminant* of the monic polynomial $f(x) = \prod (x - \alpha_j)$. Express the discriminants of the trinomials **(a)** $x^2 + px + q$, **(b)** $x^3 + px + q$, as polynomials in p, q .

Problem 3.19 Prove that the cubic trinomial $f(x) = x^3 + px + q \in \mathbb{R}[x]$ has three distinct real roots if and only if its discriminant D_f is positive. Show that in this case, there exists $\lambda \in \mathbb{R}$ such that the substitution $x = \lambda t$ reduces the equation $f(x) = 0$ to the form $4t^3 - tx = a$, where $a \in \mathbb{R}$ has $|a| \leq 1$. Use the expression for $\cos(3\varphi)$ in terms of $\cos \varphi$ from [Example 3.5](#) on p. 59 to solve $4t^3 - tx = a$ in trigonometric functions of a .

Problem 3.20 Solve the cubic equations **(a)** $x^3 - 3x + 1 = 0$, **(b)** $x^3 + x^2 - 2x - 1 = 0$, in trigonometric functions.

Problem 3.21 Find the real and imaginary parts, modulus, and argument of the following complex numbers and depict them as accurately as you can in the complex plane: **(a)** $(5 + i)(7 - 6i)/(3 + i)$, **(b)** $(1 + i)^5/(1 - i)^3$, **(c)** $\left((\sqrt{3} + i)/(1 - i)\right)^{30}$.

Problem 3.22 Using only the four arithmetic operations and square roots of positive real numbers, write explicit expressions for the real and imaginary parts of the roots of the quadratic equation $z^2 = a$.

Problem 3.23 Find all complex solutions of the following equations:

- (a)** $z^2 + (2i - 7)z + (13 - i) = 0$,
- (b)** $z^3 = i$,
- (c)** $(z + 1)^n - (z - 1)^n = 0$,
- (d)** $(z + i)^n + (z - i)^n = 0$,
- (e)** $\bar{z} = z^3$.

Problem 3.24 (Euler Product) Show that for every odd $m \in \mathbb{N}$, there exists $f_m \in \mathbb{Q}[x]$ such that $\sin mx / \sin x = f_m(\sin^2 x)$. Find the degree, roots, and leading coefficient of f_m . Show that

- (a)** $\frac{\sin(mx)}{\sin x} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \left(\sin^2 x - \sin^2 \left(\frac{2\pi j}{m} \right) \right)$,
- (b)** $(-1)^{\frac{m-1}{2}} \sin(mx) = 2^{m-1} \prod_{j=0}^{m-1} \sin \left(x + \frac{2\pi j}{m} \right)$.

Problem 3.25 For all $s, n \in \mathbb{N}$, evaluate the sum and product of the s th powers of all n th roots of unity in \mathbb{C} .

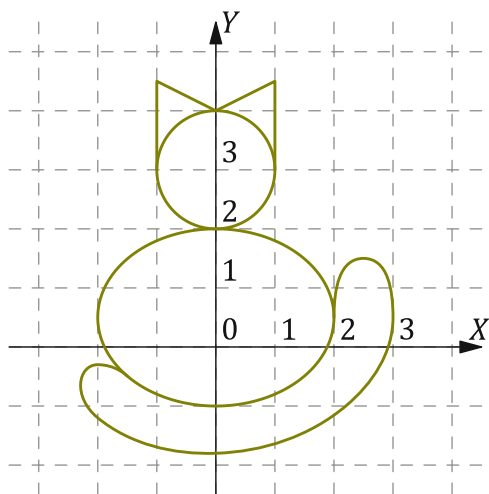
Problem 3.26 Evaluate the following sums:

- (a) $\sin x + \sin 2x + \cdots + \sin nx$,
- (b) $\cos x + 2 \cos 2x + \cdots + n \cos nx$,
- (c) $\binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \cdots$,
- (d) $\binom{n}{1} + \binom{n}{5} + \binom{n}{9} + \cdots$,
- (e) $\binom{n}{1} - \frac{1}{3}\binom{n}{5} + \frac{1}{9}\binom{n}{9} + \cdots$.

Problem 3.27 Show that three distinct points z_1, z_2, z_3 in the complex plane are collinear if and only if their *simple ratio* $(z_1 - z_3)/(z_2 - z_3)$ is real.

Problem 3.28 Show that a quadruple of distinct points $z_1, z_2, z_3, z_4 \in \mathbb{C}$ lies either on a line or on a circle if and only if their *cross ratio* $((z_1 - z_3)(z_2 - z_4)) : ((z_1 - z_4)(z_2 - z_3))$ is real.

Fig. 3.4 The complex cat



Problem 3.29 For the maps $\mathbb{C}^* \rightarrow \mathbb{C}^*$ defined by $z \mapsto z^2$ and $z \mapsto z^{-1}$, draw in the complex plane the images of (a) the line $x + y = 2$, (b) the Cartesian and polar grids, (c) the circle $|z + i| = 1$, (d) the cat in Fig. 3.4.

Problem 3.30 Write $\zeta \in \mathbb{C}$ for a primitive k th root of unity. Show that

- (a) $\prod_{v=0}^{k-1} (\zeta^v x - a) = (-1)^{k+1} (x^k - a^k)$ for all $a \in \mathbb{C}$
- (b) for every $f \in \mathbb{C}[x]$, there exists $h \in \mathbb{C}[x]$ such that $\prod_{v=0}^{k-1} f(\zeta^v x) = h(x^k)$ and the roots of h are exactly the k th powers of the roots of f .

Problem 3.31 Find a polynomial $f \in \mathbb{C}[x]$ whose complex roots are exactly

- (a) the squares of the complex roots of $x^4 + 2x^3 - x + 3$,
- (b) the cubes of the complex roots of $x^4 - x - 1$.

Problem 3.32 (Cyclotomic Polynomials) For the *cyclotomic polynomials*²⁷ $\Phi_n(x) = \prod_{\zeta}(x - \zeta)$, where $\zeta \in \mathbb{C}$ runs through the primitive n th roots of unity, show that

- (a) $\Phi_{2n}(x) = \Phi_n(-x)$ for odd n , (b) $x^n - 1 = \prod_{d|n} \Phi_d(x)$,
- (c) $\Phi_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}$,
- (d) $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ and $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$ for prime p ,
- (e) $\Phi_{pm}(x) = \Phi_m(x^p) / \Phi_m(x)$ for all $m \in \mathbb{N}$ and primes $p \nmid m$,
- (f) $\Phi_{p_1^{k_1} \cdots p_n^{k_n}}(x) = \Phi_{p_1 p_2 \cdots p_n}(x^{p_1^{k_1-1} \cdots p_n^{k_n-1}})$ for distinct primes p_i .

Problem 3.33 (Topology of the Complex Plane) An open disk of radius ε centered at a point $z \in \mathbb{C}$ is called an ε -neighborhood of z in the complex plane \mathbb{C} . The basic notions of calculus, such as the limit of a sequence of complex numbers and the limit of a function, the continuity of a function, and open and closed subsets in \mathbb{C} , are defined in terms of ε -neighborhoods in precisely the same way as those²⁸ for \mathbb{R} . Formulate and prove theorems about the limits of sums and products for convergent sequences of complex numbers. Show that $\lim_{n \rightarrow \infty} (x_n + iy_n) = a + ib$ in \mathbb{C} if and only if there exist both $\lim_{n \rightarrow \infty} x_n = a$ and $\lim_{n \rightarrow \infty} y_n = b$ in \mathbb{R} . Show that every bounded sequence of complex numbers has a convergent subsequence. Prove that for every continuous function $f : \mathbb{C} \rightarrow \mathbb{R}$ and closed, bounded subset $Z \subset \mathbb{C}$, the restriction $f|_Z : Z \rightarrow \mathbb{R}$ is bounded and achieves its maximal and minimal values at points of Z .

Problem 3.34 (Algebraic Closure of \mathbb{C}) Let $f \in \mathbb{C}[x]$ be a polynomial of positive degree. Prove that the function $|f| : \mathbb{C} \rightarrow \mathbb{R}, z \mapsto |f(z)|$, is continuous and bounded from below,²⁹ and that it achieves its minimal value on \mathbb{C} at some point $z_0 \in \mathbb{C}$. Then assume that $f(z_0) \neq 0$ and expand f as a polynomial in $w = z - z_0$: $f(z) = f(z_0) + a_m w^m + \text{higher powers of } w$, where $a_m w^m$ is the nonzero term of least positive degree. Choose some $\vartheta = \sqrt[m]{-f(z_0)/a_m} \in \mathbb{C}$ in order to have $a_m \vartheta^m = -f(z_0)$. Check that $|f(z_0 + t\vartheta)| < |f(z_0)|$ for all real t small enough. Deduce from these observations that f has a root in \mathbb{C} .

Problem 3.35 Find all invertible elements in the following rings:

- (a) $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}, i^2 = -1\}$,
- (b) $\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z}, \omega^2 + \omega + 1 = 0\}$.

²⁷See Sect. 3.5.4 on p. 60.

²⁸For example, a point $p \in \mathbb{C}$ is the *limit* of a sequence if every ε -neighborhood of p contains all but a finite number of elements of the sequence. A set U is *open* if for every $z \in U$, some ε -neighborhood of z is contained in U . A function $f : \mathbb{C} \rightarrow \mathbb{C}$ (or function $g : \mathbb{C} \rightarrow \mathbb{R}$) is *continuous* if the preimages of all open sets are open.

²⁹Hint: First show that $\forall M \in \mathbb{R}, \exists R > 0 : |f(z)| > M$ as soon as $|z| > R$.

Problem 3.36 In the ring $\mathbb{Z}[i]$, write $5 \in \mathbb{Z}[i]$ as a product of two irreducible factors.³⁰

Problem 3.37 Prove that the following properties of a prime number $p \in \mathbb{N}$ are equivalent:

- (a) $p \not\equiv 3 \pmod{4}$, (b) -1 is a square in \mathbb{F}_p , (c) p is reducible in $\mathbb{Z}[i]$,
- (d) there exists a nonzero ring homomorphism $\mathbb{Z}[i] \rightarrow \mathbb{F}_p$,
- (e) $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

Problem 3.38 (Eisenstein's Proof of Quadratic Reciprocity) Show that for every prime $p \in \mathbb{N}$, the Legendre–Jacobi symbol³¹ $\left(\frac{n}{p}\right)$ is a multiplicative character³² of n and evaluate $\sum_{n=1}^{p-1} \left(\frac{n}{p}\right)$. Then compare the sign of $\left(\frac{m}{p}\right)$ with the sign of the product

$$\prod_{j=1}^{(p-1)/2} \frac{\sin(2\pi mj/p)}{\sin(2\pi j/p)}.$$

Then take $m = q$ in this product, factorize each fraction as in [Problem 3.24](#) on p. 68, and prove that for every prime $q \in \mathbb{N}$,

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

Problem 3.39 Evaluate $\left(\frac{43}{109}\right)$.

³⁰Recall that a noninvertible element a in a commutative ring with unit is *reducible* if $a = bc$ for some noninvertible b, c ; otherwise, a is *irreducible*.

³¹See formula (3.22) on p. 65.

³²See [Problem 2.18](#) on p. 39.

Chapter 4

Elementary Functions and Power Series Expansions

In this chapter as in Chap. 3, we write K for an arbitrary commutative ring with unit and \mathbb{k} for an arbitrary field.

4.1 Rings of Fractions

4.1.1 Localization

The concept of a *fraction*,¹ which creates a field \mathbb{Q} from the ring \mathbb{Z} , is applicable in great generality. In this section, we formalize this notion for an arbitrary commutative ring K with unit.

A subset $S \subset K$ is called *multiplicative* if $1 \in S$, $0 \notin S$, and $st \in S$ for all $s, t \in S$. For example, if $q \in K$ is not nilpotent, then the set of all its nonnegative integer powers² q^k is clearly multiplicative. Another important example of a multiplicative subset is provided by the set of all elements in K that do not divide zero:

$$K^\circ \stackrel{\text{def}}{=} \{a \in K \mid ab = 0 \Rightarrow b = 0\}.$$

In particular, the nonzero elements of an integral domain form a multiplicative set.

Given a multiplicative subset $S \subset K$, write \sim_S for the equivalence on $K \times S$ generated by all relations $(a, t) \sim (as, ts)$, where $s \in S$. The equivalence class of a pair (a, s) modulo \sim_S is called a *fraction with denominator in S* and is denoted by a/s . We write KS^{-1} for the set of all such fractions and call it the *localization of K in S* or the *ring of fractions* with numerators in K and denominators in S . The appropriateness of the term “ring” is provided by Lemma 4.2 below.

¹See Example 1.5 on p. 9 and Example 2.2 on p. 20.

²By definition, we put $q^0 \stackrel{\text{def}}{=} 1$.

Lemma 4.1 *The equality $a/r = b/t$ in KS^{-1} holds if and only if there exists $s \in S$ such that $ats = brs$ in K .*

Proof Let us provisionally write $(a, r) \approx (b, t)$ if $ats = brs$ for some $s \in S$. This relation is contained in \sim_S , because it can be achieved in two steps by means of the relations generating \sim_S as follows: $(a, r) \sim (ats, rts) = (brs, rts) \sim (b, t)$. Therefore, it remains to verify that \approx is an equivalence relation. Reflexivity and symmetry are evident. Let us check transitivity. If $(a, r) \approx (b, t)$ and $(b, t) \approx (c, u)$, i.e., there are $s_1, s_2 \in S$ such that $ats_1 = brs_1$ and $bus_2 = cts_2$, then $au(ts_1s_2) = brus_1s_2 = cr(ts_1s_2)$, that is, $(a, r) \approx (c, u)$. \square

Lemma 4.2 *Addition and multiplication of fractions are well defined by the rules*

$$\frac{a}{r} + \frac{b}{s} \stackrel{\text{def}}{=} \frac{as + br}{rs}, \quad \frac{a}{r} \cdot \frac{b}{s} \stackrel{\text{def}}{=} \frac{ab}{rs}, \quad (4.1)$$

and they provide KS^{-1} with the structure of a commutative ring with unit element $1/1$ and zero element $0/1$.

Proof The consistency of the definitions (4.1) means that the results of the operations are unchanged after replacement of $\frac{a}{r}$ and $\frac{b}{s}$ by $\frac{au}{ru}$ and $\frac{bw}{sw}$ respectively, where $u, w \in S$. This is obvious:

$$\begin{aligned} \frac{au}{ru} + \frac{bw}{sw} &= \frac{ausw + bwru}{rusw} = \frac{(as + br) \cdot wu}{rs \cdot wu} = \frac{as + br}{rs}, \\ \frac{au}{ru} \cdot \frac{bw}{sw} &= \frac{aubw}{rusw} = \frac{(ab) \cdot wu}{rs \cdot wu} = \frac{ab}{rs}. \end{aligned}$$

The axioms of a commutative ring with unit are checked in the same straightforward way, and we leave this task to the reader. \square

Theorem 4.1 *The map $\iota_S : K \rightarrow KS^{-1}$, $a \mapsto a/1$, is a ring homomorphism with kernel $\ker \iota_S = \{a \in K \mid \exists s \in S : as = 0\}$. Every element of $\iota_S(S)$ is invertible in KS^{-1} . For every ring homomorphism $\varphi : K \rightarrow R$ such that $\varphi(1) = 1$ and all elements of $\varphi(S)$ are invertible in R , there exists a unique ring homomorphism $\varphi_S : KS^{-1} \rightarrow R$ such that $\varphi = \varphi_S \circ \iota_S$.*

Proof It is clear that ι_S respects both ring operations. Given $s \in S$, the inverse to $\iota_S(s) = s/1$ is $1/s$. The fraction $\iota_S(a) = a/1$ equals $0/1$ if and only if there exists $s \in S$ such that $a \cdot 1 \cdot s = 0 \cdot 1 \cdot s = 0$. It remains to prove the last statement. There is just one way to extend $\varphi : K \rightarrow R$ to a ring homomorphism $\varphi_S : KS^{-1} \rightarrow R$, because the equalities $\varphi_S(1/s) \cdot \varphi(s) = \varphi_S(s \cdot (1/s)) = \varphi_S(1) = 1$ force us to put $\varphi_S(1/s) = 1/\varphi(s)$. Therefore, the required extension should be defined by

$$\varphi_S(a/r) \stackrel{\text{def}}{=} \varphi(a) \cdot \frac{1}{\varphi(r)}.$$

This definition is consistent, because the replacement of $\frac{a}{r}$ by $\frac{as}{rs}$ for $s \in S$ leads to

$$\varphi_S\left(\frac{as}{rs}\right) = \frac{\varphi(as)}{\varphi(rs)} = \frac{\varphi(a)\varphi(s)}{\varphi(r)\varphi(s)} = \frac{\varphi(a)}{\varphi(r)}.$$

We ask the reader to check that φ_S respects addition and multiplication. \square

Remark 4.1 (Universal Property of Localization) The last statement in Theorem 4.1 is known as the *universal property* of localization. The ring KS^{-1} together with the homomorphism $\iota_S : K \rightarrow KS^{-1}$ is uniquely determined by this property in the following sense. Let a homomorphism $\iota' : K \rightarrow F$ respect the unit element and take all elements of S to invertible elements in F . If for a ring homomorphism $\varphi : K \rightarrow R$ such that $\varphi(1) = 1$ and all elements of $\varphi(S)$ are invertible in R there exists a unique ring homomorphism $\varphi' : F \rightarrow R$ such that $\varphi = \varphi' \circ \iota'$, then there exists a unique isomorphism of rings $\psi : KS^{-1} \simeq F$ such that $\iota' = \psi \circ \iota_S$. Indeed, by Theorem 4.1, the homomorphism ι' is uniquely factorized as $\iota' = \psi \circ \iota_S$. As soon as ι' also possesses the universal property, the homomorphism ι_S is also uniquely factorized as $\iota_S = \psi' \circ \iota'$. The composition $\psi' \circ \psi$ provides ι_S itself with the factorization $\iota_S = \psi' \circ \psi \circ \iota_S$. Since $\iota_S = \text{Id}_{KS^{-1}} \circ \iota_S$ as well, the uniqueness of such a factorization forces $\psi' \circ \psi = \text{Id}_{KS^{-1}}$. For the same reason, $\psi \circ \psi' = \text{Id}_F$. Thus ψ' and ψ are ring isomorphisms that are inverse to each other.

Remark 4.2 (Multiplicative Sets Containing Zero) If we remove the condition $0 \notin S$ from the definition of multiplicative set, then everything said before maintains its formal sense. The equivalence \sim_S and the ring KS^{-1} remain well defined; Lemma 4.1, Lemma 4.2, and Theorem 4.1 together with their proofs are still true as well. However, if $0 \in S$, then KS^{-1} becomes the zero ring, because of

$$a/s = (a \cdot 0)/(s \cdot 0) = 0/0 = (0 \cdot 1)/(0 \cdot 1) = 0/1$$

for every fraction a/s .

4.1.2 Field of Fractions of an Integral Domain

If K has no zero divisors, then all nonzero elements of K form a multiplicative system. The localization of K in this system is a field. It is called the *field of fractions* of K and is denoted by Q_K . The homomorphism $\iota : K \hookrightarrow Q_K$, $a \mapsto a/1$, is injective in this case. The universal property of localization says that for every ring homomorphism $\varphi : K \rightarrow R$ such that $\varphi(1) = 1$ and such that for every $a \neq 0$, $\varphi(a)$ is invertible in R , there exists a unique injection $\tilde{\varphi} : Q_K \hookrightarrow R$ coinciding with φ on $K \subset Q_K$.

Example 4.1 (The Field \mathbb{Q} Revisited) The field of fractions of \mathbb{Z} is the field of rational numbers $\mathbb{Q}_{\mathbb{Z}} = \mathbb{Q}$. It is canonically embedded as the prime subfield into any field of zero characteristic.³

Example 4.2 (Laurent Series) For a field \mathbb{k} , the ring of formal power series $\mathbb{k}[[x]]$ is an integral domain. Its field of fractions $\mathbb{Q}_{\mathbb{k}[[x]]}$ is described as follows. Every power series $q(x) \in \mathbb{k}[[x]]$ can be uniquely written as $x^m q_{\text{red}}(x)$, where m equals the degree of the lowest term in q , and $q_{\text{red}} \in \mathbb{k}[[x]]$ has nonzero constant term. Since every power series with nonzero constant term is invertible in $\mathbb{k}[[x]]$, every fraction $f = p/q$ can be uniquely written as $f = x^{-m}p/q_{\text{red}} = x^{-m}h$, where $h \in \mathbb{k}[[x]]$. We conclude that the field of fractions $\mathbb{Q}_{\mathbb{k}[[x]]}$ coincides with the localization of $\mathbb{k}[[x]]$ in the multiplicative system of powers x^m . The latter consists of formal power series with integer exponents bounded from below:

$$f(x) = \sum_{k \geq -m} a_k x^k = a_{-m} x^{-m} + \cdots + a_{-1} x^{-1} + a_0 + a_1 x + a_2 x^2 + \cdots. \quad (4.2)$$

It is denoted by $\mathbb{k}((x))$ and is called the field of *Laurent series*. Thus, $\mathbb{Q}_{\mathbb{k}[[x]]} \simeq \mathbb{k}((x))$.

4.2 Field of Rational Functions

4.2.1 Simplified Fractions

The field of fractions of the polynomial ring $\mathbb{k}[x]$ is denoted by $\mathbb{k}(x)$ and is called the *field of rational functions* in one variable. The elements of $\mathbb{k}[x]$ are the fractions

$$f(x) = p(x)/q(x), \text{ where } p, q \in \mathbb{k}[x], q \neq 0. \quad (4.3)$$

Every fraction admits many different representations (4.3) as a ratio of two polynomials. Among these, there is a minimal one, called *simplified*, which has a monic denominator that is coprime to the numerator. It is obtained from (4.3) by cancellation of $\text{GCD}(p, q)$ and the leading coefficient of q .

Exercise 4.1 Show that two fractions are equal in $\mathbb{k}(x)$ if and only if their simplified representations coincide.

Proposition 4.1 Assume that the denominator of the simplified representation f/g is factorized as $g = g_1 \cdot g_2 \cdots g_m$, where $\text{GCD}(g_i, g_j) = 1$ for all $i \neq j$ and all g_i are monic. Then the fraction f/g is uniquely expanded in $\mathbb{k}(x)$ as a sum of simplified

³See Sect. 2.8 on p. 35.

fractions

$$\frac{f}{g} = h + \frac{f_1}{g_1} + \frac{f_2}{g_2} + \cdots + \frac{f_m}{g_m}, \quad (4.4)$$

where $\deg h = \deg f - \deg g$ and $\deg f_i < \deg g_i$ for all i .

Proof Write $G_i = g/g_i$ for the product of all g_i except g_i . Then (4.4) is equivalent to

$$f = hg + f_1G_1 + f_2G_2 + \cdots + f_mG_m,$$

where $\deg(f_1G_1 + f_2G_2 + \cdots + f_mG_m) < \deg g$, because of the above assumptions on the degrees. This means that h is the quotient of the division of f by g , $f_1G_1 + f_2G_2 + \cdots + f_mG_m$ is the remainder of this division, and each f_i is the unique polynomial of degree $\deg f_i < \deg g_i$ that represents the residue class $[f] \cdot [G_i]^{-1}$ in $\mathbb{k}[x]/(g_i)$. Thus, all ingredients of (4.4) exist and are uniquely determined by f and g_1, g_2, \dots, g_n . \square

Proposition 4.2 *Every simplified fraction f/g^m , where $\deg f < \deg(g^m)$ and g is monic, is uniquely expanded in $\mathbb{k}(x)$ as a sum of simplified fractions*

$$\frac{f}{g^m} = \frac{f_1}{g} + \frac{f_2}{g^2} + \cdots + \frac{f_m}{g^m}, \quad (4.5)$$

where $\deg f_i < \deg g$ for all i .

Proof The expansion (4.5) is equivalent to the expansion

$$f = f_1g^{m-1} + f_2g^{m-2} + \cdots + f_{m-1}g + f_m, \quad (4.6)$$

which is nothing but the representation of f in g -adic notation, where f_m is the remainder on division of f by g , f_{m-1} is the remainder on division of the quotient $(f - f_m)/g$ by g , f_{m-2} is the remainder on division of the quotient $((f - f_m)/g - f_{m-1})/g$ by g , etc. \square

4.2.2 Partial Fraction Expansion

The two previous lemmas imply that every simplified fraction $f/g \in \mathbb{k}(x)$ can be uniquely written as a sum of a polynomial of degree $\deg f - \deg g$ and a number of simplified fractions p/q^m , where $\deg p < \deg q$, q runs through the monic irreducible divisors of g , and $m \in \mathbb{N}$ varies between 1 and the multiplicity of q in the irreducible factorization of g . This sum is called the *partial fraction expansion* of f/g . It can be helpful in practical computations.

Example 4.3 Let us compute the antiderivative⁴ and 2016th derivative of $1/(1+x^2)$. The partial fraction expansion of $1/(1+x^2)$ in $\mathbb{C}(x)$ looks like

$$\frac{1}{1+x^2} = \frac{\alpha}{1+ix} + \frac{\beta}{1-ix}, \text{ where } \alpha, \beta \in \mathbb{C}.$$

Substituting $x = \pm i$ in the equality $1 = \alpha(1-ix) + \beta(1+ix)$, we conclude that $\alpha = \beta = 1/2$, i.e.,

$$\frac{1}{1+x^2} = \frac{1}{2} \left(\frac{1}{1+ix} + \frac{1}{1-ix} \right).$$

Now we can easily compute the 2016th derivative,

$$\begin{aligned} \left(\frac{d}{dx} \right)^{2016} \frac{1}{1+x^2} &= \frac{1}{2} \left(\frac{d}{dx} \right)^{2016} (1+ix)^{-1} + \frac{1}{2} \left(\frac{d}{dx} \right)^{2016} (1-ix)^{-1} \\ &= \frac{2015!}{2} ((1+ix)^{-2016} + (1-ix)^{-2016}) \\ &= \frac{2015!}{(1+x^2)^{2016}} \cdot \frac{(1-ix)^{2016} + (1+ix)^{2016}}{2} \\ &= \frac{2015!}{(1+x^2)^{2016}} \cdot \left(1 - \binom{2016}{2} x^2 + \binom{2016}{4} x^4 - \binom{2016}{6} x^6 + \dots \right. \\ &\quad \left. - \binom{2016}{2} x^{2104} + x^{2016} \right), \end{aligned}$$

as well as the antiderivative,

$$\begin{aligned} \int \frac{dx}{1+x^2} &= \frac{1}{2} \int \frac{dx}{1+ix} + \frac{1}{2} \int \frac{dx}{1-ix} \\ &= \frac{1}{2} (\log(1+ix) + \log(1-ix)) = \log \sqrt{1+x^2}. \end{aligned}$$

All these equalities can in fact be treated purely algebraically within the ring $\mathbb{K}[[x]]$. In the next sections, we shall explain explicitly what this means.

⁴It will be defined explicitly in Sect. 4.3 on p. 82.

4.2.3 Power Series Expansions of Rational Functions

By the universal property of localization, the tautological inclusion $\mathbb{k}[x] \subset \mathbb{k}((x))$ can be uniquely extended to the inclusion of fields

$$\mathbb{k}(x) \hookrightarrow \mathbb{k}((x)),$$

which is the identity on the subring of polynomials. From a practical viewpoint, this means that each rational function f/g can be uniquely expanded as a Laurent power series. Such an expansion can be made quite explicit as soon as the denominator g is completely factorized into linear binomials.⁵ Let $\deg f < \deg g$ and

$$g(x) = 1 + a_1x + a_2x^2 + \cdots + a_nx^n = \prod (1 - \alpha_i x)^{m_i}, \quad (4.7)$$

where all $\alpha_i \in \mathbb{k}$ are distinct and $a_n \neq 0$.

Exercise 4.2 Check that the numbers α_i on the right-hand side of (4.7) are roots of the polynomial

$$\chi(t) = t^n g(1/t) = t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n = \prod (t - \alpha_i)^{m_i}. \quad (4.8)$$

Then the partial fraction expansion of f/g consists of fractions

$$\frac{\beta_{ij}}{(1 - \alpha_i x)^{k_{ij}}}, \quad (4.9)$$

where $\beta_{ij} \in \mathbb{k}$ and $1 \leq k_{ij} \leq m_i$ for each i . When all the multiplicities m_i are equal to 1, the partial fraction expansion takes the especially simple form

$$\frac{f(x)}{(1 - \alpha_1 x)(1 - \alpha_2 x) \cdots (1 - \alpha_n x)} = \frac{\beta_1}{1 - \alpha_1 x} + \frac{\beta_2}{1 - \alpha_2 x} + \cdots + \frac{\beta_n}{1 - \alpha_n x}. \quad (4.10)$$

The constants β_i can be found via multiplication of both sides by the common denominator and substituting $x = \alpha_i^{-1}$. This leads to

$$\beta_i = \frac{f(\alpha_i^{-1})}{\prod_{v \neq i} (1 - (\alpha_v / \alpha_i))} = \frac{\alpha_i^{n-1} f(\alpha_i^{-1})}{\prod_{v \neq i} (\alpha_i - \alpha_v)}. \quad (4.11)$$

⁵Such a factorization is always possible (at least in theory) over an algebraically closed field \mathbb{k} (see Sect. 3.4.3 on p. 55).

Exercise 4.3 Check that $1/(1-\alpha x) = 1 + \alpha x + \alpha^2 x^2 + \cdots = \sum_{k \geq 0} \alpha^k x^k$ in $\mathbb{K}[[x]]$.

Therefore, if all m_i are equal to 1, then the fraction f/g is the sum of geometric progressions (4.10):

$$f(x)/g(x) = \sum_{k \geq 0} (\beta_1 \alpha_1^k + \beta_2 \alpha_2^k + \cdots + \beta_n \alpha_n^k) \cdot x^k,$$

where the β_i are provided by formula (4.11). If there are some $\beta/(1-\alpha x)^m$ with $m > 1$ among the partial fractions (4.9), then they are expanded in power series by Newton's binomial formula with *negative* integer exponent:

$$\frac{1}{(1-x)^m} = \sum_{k \geq 0} \frac{(k+m-1)(k+m-2) \cdots (k+1)}{(m-1)!} \cdot x^k = \sum_{k \geq 0} \binom{k+m-1}{m-1} \cdot x^k, \quad (4.12)$$

obtained by $(m-1)$ -fold differentiation of both sides in $(1-x)^{-1} = 1 + x + x^2 + x^3 + x^4 + \cdots$.

Exercise 4.4 Check that $(\frac{d}{dx})^m (1-x)^{-1} = m!/(1-x)^{m+1}$.

Thus, a partial fraction with multiple denominator is expanded as

$$\frac{\beta}{(1-\alpha_i x)^m} = \beta \sum_{k \geq 0} \alpha_i^k \binom{k+m-1}{m-1} \cdot x^k. \quad (4.13)$$

4.2.4 Linear Recurrence Relations

A linear recurrence of order n on a sequence $z_k \in \mathbb{K}$ of unknowns is a relation

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \cdots + a_n z_{k-n} = 0, \quad (4.14)$$

where $a_1, a_2, \dots, a_n \in \mathbb{K}$ are given constants, and the first n terms z_0, z_1, \dots, z_{n-1} of the sequence are also known. To solve equation (4.14) means to write z_k as an explicit function of k . This can be done as follows. Consider the *generating power series* of the sequence

$$z(x) \stackrel{\text{def}}{=} z_0 + z_1 x + z_2 x^2 + \cdots = \sum_{k \geq 0} z_k x^k \in \mathbb{K}[[x]].$$

Relation (4.14) says that the product $z(x) \cdot (1 + a_1x + a_2x^2 + \cdots + a_nx^n)$ is a polynomial of degree at most $n - 1$. Hence, $z(x)$ is a power series expansion for the rational function

$$\frac{b_0 + b_1x + \cdots + b_{n-1}x^{n-1}}{1 + a_1x + a_2x^2 + \cdots + a_nx^n}. \quad (4.15)$$

The coefficients b_0, b_1, \dots, b_{n-1} are uniquely determined by the initial terms z_0, z_1, \dots, z_{n-1} by means of the equality

$$\begin{aligned} (z_0 + z_1x + \cdots + z_{n-1}x^{n-1}) \cdot (1 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}) \\ = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + \text{higher-degree terms.} \end{aligned} \quad (4.16)$$

Therefore, to write z_k as an explicit function of k , we have to compute b_0, b_1, \dots, b_{n-1} from (4.16) and expand the fraction (4.15) into a power series.

Example 4.4 (Fibonacci Numbers) Let us find the k th element of the *Fibonacci sequence* z_k defined recursively as

$$z_0 = 0, \quad z_1 = 1, \quad z_k = z_{k-1} + z_{k-2} \quad \text{for } k \geq 2.$$

This sequence satisfies a linear recurrence equation of second order: $z_k - z_{k-1} - z_{k-2} = 0$. The equality (4.16) becomes $x(1 - x - x^2) = b_0 + b_1x + \cdots$ and gives $b_0 = 0, b_1 = 1$. Thus, z_k equals the k th coefficient in the power series expansion of the rational function

$$z(x) = \frac{x}{1 - x - x^2} = \frac{\beta_+}{1 - \alpha_+x} + \frac{\beta_-}{1 - \alpha_-x},$$

where $\alpha_{\pm} = (1 \pm \sqrt{5})/2$ are the roots of the polynomial⁶ $t^2 - t - 1$, and the β_{\pm} are given by (4.11):

$$\beta_+ = \alpha_+\alpha_+^{-1}/(\alpha_+ - \alpha_-) = \frac{1}{\sqrt{5}} \quad \text{and} \quad \beta_- = \alpha_-\alpha_-^{-1}/(\alpha_- - \alpha_+) = -\frac{1}{\sqrt{5}}.$$

Hence,

$$\frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \alpha_+x} - \frac{1}{1 - \alpha_-x} \right) = \sum_{k \geq 0} \frac{\alpha_+^k - \alpha_-^k}{\sqrt{5}} \cdot x^k$$

⁶See formula (4.8) on p. 79.

and

$$z_k = \frac{(1 + \sqrt{5})^k - (1 - \sqrt{5})^k}{\sqrt{5} \cdot 2^k}.$$

Exercise 4.5 Can you show that z_k is a positive integer?

Proposition 4.3 *Let the polynomial (4.8) of the linear order- n recurrence equation $z_k + a_1 z_{k-1} + a_2 z_{k-2} + \cdots + a_n z_{k-n} = 0$, where $a_i \in \mathbb{k}$, be completely factorized in $\mathbb{k}[t]$ as $t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n = \prod_{i=1}^r (t - \alpha_i)^{m_i}$, where $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{k}$ are distinct. Then every sequence z_k satisfying this equation has the form $z_k = \alpha_1^k \cdot \varphi_1(k) + \alpha_2^k \cdot \varphi_2(k) + \cdots + \alpha_r^k \cdot \varphi_r(k)$, where each $\varphi_i(x) \in \mathbb{k}[x]$ is a polynomial of degree at most $m_i - 1$.*

Proof The generating series $\sum z_k x^k \in \mathbb{k}[[x]]$ of any solution is a power series expansion for a sum of partial fractions of the form $\beta \cdot (1 - \alpha x)^{-m}$, where α is a root of the polynomial (4.8), the integer m is in the range $1 \leq m \leq m_i$, and $\beta \in \mathbb{k}$ is some constant uniquely determined by α, m, n , and the initial terms of the sequence z_k . By formula (4.13) on p. 80, such a fraction is expanded as $\sum_{k \geq 0} \beta \cdot \alpha^k \cdot \varphi(k) \cdot x^k$, where $\varphi(k) = \binom{k+m-1}{m-1}$ is a polynomial of degree $m-1$ in k . \square

Remark 4.3 The polynomial $\chi(t) = t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n$ is called the *characteristic polynomial* of the recurrence relation $z_k + a_1 z_{k-1} + a_2 z_{k-2} + \cdots + a_n z_{k-n} = 0$. As soon as a complete linear factorization of $\chi(t)$ is known, Proposition 4.3 allows us to solve the recurrence relation via the method of undetermined coefficients: consider the coefficients of polynomials φ_v as unknowns and determine them from the initial conditions $z_i = \alpha_1^i \cdot \varphi_1(i) + \alpha_2^i \cdot \varphi_2(i) + \cdots + \alpha_r^i \cdot \varphi_r(i)$, $0 \leq i \leq n-1$, which form a system of n ordinary linear equations in n unknown coefficients.

4.3 Logarithm and Exponential

Throughout this section, we assume that \mathbb{k} is a field of characteristic zero. In this case, formula (3.7) on p. 45 for the derivative,

$$(a_0 + a_1 x + a_2 x^2 + \cdots)' = a_1 + 2 a_2 x + 3 a_3 x^2 + \cdots = \sum_{k \geq 1} k a_k x^{k-1}, \quad (4.17)$$

implies that for every power series $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in \mathbb{k}[[x]]$, there exists a unique power series $F \in \mathbb{k}[[x]]$ without constant term such that $F' = f$. This series is called the *antiderivative* of f and is denoted by

$$\int f(x) dx \stackrel{\text{def}}{=} a_0 x + \frac{a_1}{2} x^2 + \frac{a_2}{3} x^3 + \cdots = \sum_{k \geq 1} \frac{a_{k-1}}{k} x^k. \quad (4.18)$$

4.3.1 The Logarithm

The antiderivative of the alternating-sign geometric progression is called the *logarithm* and is denoted by

$$\begin{aligned}\log(1+x) &\stackrel{\text{def}}{=} \int \frac{dx}{1+x} = \int (1-x+x^2-x^3+\cdots) dx \\ &= x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \cdots = \sum_{k \geq 1} \frac{(-1)^{k-1}}{k} x^k.\end{aligned}\quad (4.19)$$

Write $N \subset \mathbb{K}[[x]]$ for the additive abelian group of all power series without constant term and $U \subset \mathbb{K}[[x]]$ for the multiplicative abelian group of all power series with constant term 1. We can replace $1+x$ in $\log(1+x)$ with any power series $u(x) \in U$. This is an algebraic operation, because it means substituting $u(x) - 1$ for x , and $u(x) - 1$ has no constant term. Therefore, taking the logarithm produces a well-defined map

$$\log : U \rightarrow N, \quad u \mapsto \log u. \quad (4.20)$$

Exercise 4.6 (Logarithmic Derivative) Verify that $\frac{d}{dx} \log u = u'/u$ for all $u \in U$.

Lemma 4.3 For all $u, w \in U$, the equalities $u = w$, $u' = w'$, $\log(u) = \log(w)$, $u'/u = w'/w$ are equivalent.

Proof The first equality implies all the others. For two power series u, w with equal constant terms, the first two equalities are equivalent by the differentiation formula (4.17). Replacing u, w by $\log u, \log w$, we get the equivalence of the last two equalities. It remains to deduce the first equality from the last. The last equality forces $0 = u'/u - w'/w = (u'w - w'u)/uw = (w/u) \cdot (u/w)'$. Thus, $(u/w)' = 0$, that is, $u/w = \text{const} = 1$. \square

Exercise 4.7 Show that $\log(1/u) = -\log u$ for all $u \in U$.

4.3.2 The Exponential

There exists a unique power series $f \in U$ such that $f' = f$. It is called the *exponential* and denoted by

$$e^x \stackrel{\text{def}}{=} \sum_{k \geq 0} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \cdots \quad (4.21)$$

We can replace x in e^x by any power series $\tau(x) \in N$. This leads to the power series $e^{\tau(x)}$ with constant term 1. Therefore, the exponential produces a well-defined map,

$$\exp : N \rightarrow U, \quad \tau \mapsto e^\tau. \quad (4.22)$$

Theorem 4.2 *The maps (4.22) and (4.20) taking the exponential and logarithm of power series*

$$\begin{array}{ccc} N & \xrightleftharpoons[\log u \mapsto u]{\tau \mapsto e^\tau} & U \end{array} \quad (4.23)$$

are isomorphisms of abelian groups each the inverse of the other. That is, the equalities

$$\log e^\tau = \tau, \quad e^{\log u} = u, \quad \log(u_1 u_2) = \log(u_1) + \log(u_2), \quad e^{\tau_1 + \tau_2} = e^{\tau_1} e^{\tau_2},$$

hold for all $u, u_1, u_2 \in U$ and all $\tau, \tau_1, \tau_2 \in N$.

Proof Differentiation of both sides immediately verifies the equality $\log e^\tau = \tau$. After that, taking the logarithms of both sides verifies the equality $e^{\log u} = u$. Therefore, the maps (4.23) are bijections that are inverses to each other. The power series $\log(u_1 u_2)$ and $\log u_1 + \log u_2$ coincide, because they have equal constant terms and equal derivatives:

$$(\log(u_1 u_2))' = \frac{(u_1 u_2)'}{u_1 u_2} = \frac{u_1' u_2 + u_1 u_2'}{u_1 u_2} = \frac{u_1'}{u_1} + \frac{u_2'}{u_2} = (\log u_1 + \log u_2)'.$$

Hence, \log is a homomorphism. This forces the inverse map to be a homomorphism as well. \square

Exercise 4.8 Prove that $e^{x+y} = e^x e^y$ in $\mathbb{k}[[x, y]]$ by straightforward comparison of the coefficients of like monomials on both sides.

4.3.3 Power Function and Binomial Formula

For $\alpha \in \mathbb{k}$, the *binomial series* with exponent α is defined as

$$(1+x)^\alpha \stackrel{\text{def}}{=} e^{\alpha \log(1+x)}.$$

In this formula, $1+x$ can be replaced by any power series $u \in U$. Thus, for every $\alpha \in \mathbb{k}$ there is an algebraic operation $U \rightarrow U$, $u \mapsto u^\alpha$, called the *power function*

with exponent α . It satisfies the expected list of properties: for all $u, v \in U$ and all $\alpha, \beta \in \mathbb{K}$, we have

$$u^\alpha \cdot u^\beta = e^{\alpha \log u} \cdot e^{\beta \log u} = e^{\alpha \log u + \beta \log u} = e^{(\alpha+\beta) \log u} = u^{\alpha+\beta}, \quad (4.24)$$

$$(u^\alpha)^\beta = e^{\beta \log(u^\alpha)} = e^{\beta \log(e^{\alpha \log u})} = e^{\alpha\beta \log u} = u^{\alpha\beta}, \quad (4.25)$$

$$(uv)^\alpha = e^{\alpha \log(uv)} = e^{\alpha(\log u + \log v)} = e^{\alpha \log u + \alpha \log v} = e^{\alpha \log u} \cdot e^{\alpha \log v} = u^\alpha v^\alpha. \quad (4.26)$$

In particular, $u^{1/n} = \sqrt[n]{u}$ for every $u \in U$ in the sense that $(u^{1/n})^n = u$.

To find the coefficients of the binomial $(1+x)^\alpha = 1 + a_1x + a_2x^2 + \dots$ explicitly, let us take the logarithmic derivative of both sides. This gives

$$\frac{\alpha}{1+x} = \frac{a_1 + 2a_2x + 3a_3x^2 + \dots}{1 + a_1x + a_2x^2 + \dots}.$$

Thus, $\alpha \cdot (1 + a_1x + a_2x^2 + \dots) = (1+x) \cdot (a_1 + 2a_2x + 3a_3x^2 + \dots)$. Therefore, $a_1 = \alpha$ and $\alpha a_{k-1} = ka_k + (k-1)a_{k-1}$ for $k \geq 2$. This leads to

$$\begin{aligned} a_k &= \frac{\alpha - (k-1)}{k} \cdot a_{k-1} = \frac{(\alpha - (k-1))(\alpha - (k-2))}{k(k-1)} \cdot a_{k-2} = \dots \\ &= \frac{(\alpha - (k-1))(\alpha - (k-2)) \dots (\alpha - 1)\alpha}{k!}. \end{aligned}$$

Both the numerator and denominator of the last fraction consist of k factors decreasing by 1 from k to 1 in the denominator and from α to $\alpha - k + 1$ in the numerator. This fraction is denoted by

$$\binom{\alpha}{k} \stackrel{\text{def}}{=} \frac{\alpha(\alpha-1) \dots (\alpha-k+1)}{k!} \quad (4.27)$$

and called the *binomial coefficient* of the exponent $\alpha \in \mathbb{K}$. We make the following claim.

Proposition 4.4 (Newton's Binomial Formula) *For every $\alpha \in \mathbb{K}$, there exists a formal power series expansion*

$$(1+x)^\alpha = \sum_{k \geq 0} \binom{\alpha}{k} x^k = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2} x^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{6} x^3 + \dots. \quad (4.28)$$

Example 4.5 (Binomial with Rational Exponent) If the exponent α is equal to $n \in \mathbb{N}$, then the numerator (4.27) acquires zero factors for all $k > n$, and the binomial expansion (4.28) becomes finite:

$$(1+x)^n = 1 + nx + \frac{n(n-1)}{2}x^2 + \cdots + x^n = \sum_{k=0}^n \binom{n}{k} \cdot x^k.$$

This agrees with formula (1.7) on p. 6. If $\alpha = -m$ is a negative integer, then the expansion (4.28) turns into the one obtained in formula (4.12) on p. 80:

$$\begin{aligned} (1+x)^{-m} &= 1 - mx + \frac{m(m+1)}{2}x^2 - \frac{m(m+1)(m+2)}{6}x^3 + \cdots \\ &= \sum_{k \geq 0} (-1)^k \binom{k+m-1}{k} \cdot x^k. \end{aligned}$$

For $\alpha = 1/n$, $n \in \mathbb{N}$, the binomial formula (4.28) expands the *radical function*

$$\begin{aligned} \sqrt[n]{1+x} &= 1 + \frac{1}{n}x + \frac{\frac{1}{n}(\frac{1}{n}-1)}{2}x^2 + \frac{\frac{1}{n}(\frac{1}{n}-1)(\frac{1}{n}-2)}{6}x^3 + \cdots \\ &= 1 + \frac{x}{n} - \frac{n-1}{2} \cdot \frac{x^2}{n^2} + \frac{(n-1)(2n-1)}{2 \cdot 3} \cdot \frac{x^3}{n^3} \\ &\quad - \frac{(n-1)(2n-1)(3n-1)}{2 \cdot 3 \cdot 4} \cdot \frac{x^4}{n^4} + \cdots. \end{aligned}$$

For example, when $n = 2$, the coefficient of x^k equals

$$\begin{aligned} (-1)^{k-1} \cdot \frac{1 \cdot 3 \cdot 5 \cdots (2k-3)}{2 \cdot 4 \cdot 6 \cdots (2k)} &= \frac{(-1)^{k-1}}{2k-1} \cdot \frac{(2k)!}{(2 \cdot 4 \cdot 6 \cdots (2k))^2} \\ &= \frac{(-1)^{k-1}}{(2k-1) \cdot 4^k} \cdot \binom{2k}{k}. \end{aligned}$$

Thus,

$$\sqrt{1+x} = \sum_{k \geq 0} \frac{(-1)^{k-1}}{2k-1} \cdot \binom{2k}{k} \cdot \frac{x^k}{4^k}. \quad (4.29)$$

Example 4.6 (Catalan Numbers) Let us use the square root expansion (4.29) to deduce an explicit formula for the Catalan numbers, which appear in many combinatorial problems. The product of $(n+1)$ quantities

$$a_0 a_1 a_2 \cdots a_n \quad (\text{an } n\text{-fold product}) \quad (4.30)$$

can be computed in n steps by executing one multiplication per step. If in each step, we enclose the items to be multiplied in parentheses, then the entire computation will be encoded by n pairs of parentheses inserted into (4.30). For $n = 1$, there is just one arrangement of parentheses: (a_1a_2) ; for $n = 2$, there are two: $(a_1(a_2a_3))$ and $((a_1a_2)a_3)$; for $n = 3$, there are five:

$$(a_1(a_2(a_3a_4))), (a_1((a_2a_3)a_4)), ((a_1a_2)(a_3a_4)), ((a_1(a_2a_3))a_4), (((a_1a_2)a_3)a_4).$$

We see that not all $n!$ combinations of n sequential multiplications appear in the step-by-step evaluation of (4.30). The total number of admissible distributions of n pairs of parentheses in (4.30) provided by all evaluations of the product is called the n th *Catalan number* and is denoted by c_n . It is also convenient to put $c_0 \stackrel{\text{def}}{=} 1$. The next few values are $c_1 = 1, c_2 = 2, c_3 = 5$.

For $n \geq 2$, the set of all admissible arrangements of n pairs of parentheses splits into n disjoint classes in accordance with the position of the penultimate pair of parentheses:

$$(a_0(a_2 \dots a_n)), ((a_0a_1)(a_2 \dots a_n)), ((a_0a_1a_2)(a_3 \dots a_n)), ((a_0 \dots a_3)(a_4 \dots a_n)), \dots, ((a_0 \dots a_{n-3})(a_{n-2}a_{n-1}a_n)), ((a_0 \dots a_{n-2})(a_{n-1}a_n)), ((a_0 \dots a_{n-1})a_n).$$

The classes consist of $c_{n-1}, c_1c_{n-2}, c_2c_{n-3}, c_3c_{n-4}, \dots, c_{n-2}c_1, c_{n-1}c_0$ elements respectively. Therefore the Catalan numbers satisfy the recurrence

$$c_n = c_0c_{n-1} + c_1c_{n-2} + \dots + c_{n-2}c_1 + c_{n-1}c_0,$$

which says that the *Catalan power series*

$$c(x) = \sum_{k \geq 0} c_k x^k = 1 + c_1x + c_2x^2 + c_3x^3 + \dots \in \mathbb{Z}[[x]]$$

satisfies the relation $c(x)^2 = (c(x) - 1)/x$. In other words, $t = c(x)$ is a root of the quadratic polynomial $x \cdot t^2 - t - 1 = 0$ in t with coefficients in the field of Laurent series $\mathbb{Q}((x))$. By the famous quadratic formula, the two roots of this polynomial are

$$\frac{1 \pm \sqrt{1 - 4x}}{2x}. \quad (4.31)$$

Since

$$\sqrt{1 - 4x} = - \sum_{k \geq 0} \frac{1}{2k - 1} \cdot \binom{2k}{k} \cdot x^k = 1 - 2x - 2x^2 - 4x^3 - 10x^4 - \dots,$$

and we are looking for the root living in the subring $\mathbb{Z}[[x]] \subset \mathbb{Q}((x))$, we have to choose the minus sign in (4.31). Thus, $c(x) = (1 - \sqrt{1 - 4x})/(2x)$, and we conclude

from (4.29) that

$$c_k = \frac{1}{2} \cdot \frac{1}{2k+1} \cdot \binom{2k+2}{k+1} = \frac{1}{k+1} \cdot \binom{2k}{k}.$$

Exercise 4.9 Can you show that c_k is an integer?

4.4 Todd's Series and Bernoulli Numbers

4.4.1 Action of $\mathbb{Q}[[d/dt]]$ on $\mathbb{Q}[t]$

Consider the ring of formal power series $\mathbb{Q}[[x]]$ in the variable x and the ring of polynomials $\mathbb{Q}[t]$ in the variable t , and write

$$D = \frac{d}{dt} : \mathbb{Q}[t] \rightarrow \mathbb{Q}[t], \quad g \mapsto g',$$

for the differentiation operator acting on $\mathbb{Q}[t]$. We can substitute D for x in any formal power series $\Phi(x) = \sum_{k \geq 0} \varphi_k x^k \in \mathbb{Q}[[x]]$ and treat the result as a map

$$\Phi(D) : \mathbb{Q}[t] \rightarrow \mathbb{Q}[t], \quad f \mapsto \varphi_0 \cdot f + \varphi_1 \cdot f' + \varphi_2 \cdot f'' + \cdots = \sum_{k \geq 0} \varphi_k \cdot D^k f. \quad (4.32)$$

Since each differentiation decreases the degree of a polynomial by 1, all summands with $k > \deg f$ vanish. Therefore, for every $f \in \mathbb{Q}[t]$, the right-hand side of (4.32) is a well-defined polynomial of degree equal to at most $\deg f$. We write $\Phi(D)f$ for this polynomial. Note that its coefficients are polynomials in the coefficients of f and the first $\deg(f)$ coefficients of Φ . Moreover, $\Phi(D)f$ is *linear homogeneous* in f in the sense that

$$\forall \alpha, \beta \in \mathbb{Q} \quad \forall f, g \in \mathbb{Q}[t], \quad \Phi(D)(\alpha \cdot f + \beta \cdot g) = \alpha \cdot \Phi(D)f + \beta \cdot \Phi(D)g, \quad (4.33)$$

because the derivation operator D and all its iterations D^k are linear homogeneous. Note also that after the substitution $x = D$ in the product of power series $\Phi(x)\Psi(x) \in \mathbb{Q}[[x]]$, we get the *composition* of maps $\Phi(D) \circ \Psi(D)$.

Exercise 4.10 Check all these claims.

Hence, all maps $\Phi(D)$ commute with each other. Any two maps $\Phi(D)$, $\Phi^{-1}(D)$ resulting from inverse elements Φ , $\Phi^{-1} = 1/\Phi$ of $\mathbb{Q}[[x]]$ are mutually inverse bijective maps. Therefore, the operators $\Phi(D)$, $\Phi \in \mathbb{Q}[[x]]$, form an abelian transformation group of $\mathbb{Q}[t]$ in the sense of Example 1.7 on p. 13.

The linearity of $\Phi(D)f$ in f allows us to compute $\Phi(D)f$ for every f as soon as the sequence of polynomials $\Phi_m(t) \stackrel{\text{def}}{=} \Phi(D)t^m$ is known. For

$$f(t) = a_0 t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n,$$

we get

$$\Phi(D)(a_0 + a_1 t + \cdots + a_n t^n) = a_0 + a_1 \Phi_1(t) + a_2 \Phi_2(t) + \cdots + a_n \Phi_n(t).$$

The polynomial $\Phi_m \in \mathbb{Q}[t]$ is called the *mth Appell polynomial* of the power series $\Phi \in \mathbb{Q}[[x]]$. It depends only on the first $m + 1$ coefficients of Φ and has degree at most m .

Example 4.7 (Shift Operators) The Appell polynomials of exponent $e^x = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \cdots$ are

$$\begin{aligned} e^D t^m &= \sum_{k \geq 0} \frac{1}{k!} D^k t^m = \sum_{k \geq 0} \frac{m(m-1) \cdots (m-k+1)}{k!} t^{m-k} \\ &= \sum_{k=0}^m \binom{m}{k} t^{m-k} = (t+1)^m. \end{aligned}$$

Hence, the operator e^D acts on $\mathbb{Q}[t]$ as the *shift of variable* $e^D : f(t) \mapsto f(t+1)$. Since the series e^{-x} is inverse to e^x in $\mathbb{Q}[[x]]$, the operator e^{-D} acts as the inverse shift $e^{-D} : f(t) \mapsto f(t-1)$.

Exercise 4.11 Check that $e^{\alpha D} : f(t) \mapsto f(t+\alpha)$ for all $\alpha \in \mathbb{Q}$.

Example 4.8 (Power Sums of Integers) We are looking for polynomials $S_m(t) \in \mathbb{Q}[t]$, numbered by integers $m \geq 0$, such that

$$S_m(n) = 0^m + 1^m + 2^m + 3^m + \cdots + n^m = \sum_{k=0}^n k^m \quad (4.34)$$

for all integers $n \geq 0$. For example, for $m = 0, 1, 2, 3$, we have the well-known formulas⁷

$$\begin{aligned} S_0(n) &= 1 + 1 + 1 + \cdots + 1 = n, \\ S_1(n) &= 1 + 2 + 3 + \cdots + n = n(n+1)/2, \\ S_2(n) &= 1^2 + 2^2 + 3^2 + \cdots + n^2 = n(n+1)(2n+1)/6, \\ S_3(n) &= 1^3 + 2^3 + 3^3 + \cdots + n^3 = n^2(n+1)^2/4 = S_1(n)^2, \end{aligned} \quad (4.35)$$

⁷Do not worry if you are not conversant with some of them. We will deduce them all soon.

which mean that $S_0(t) = t$, $S_1(t) = t(t+1)/2$, $S_2(t) = t(t+1)(2t+1)/6$, $S_3 = S_1^2$. To analyze the general case, let us consider the *difference operator* $\nabla = 1 - e^{-D}$: $\varphi(t) \mapsto \varphi(t) - \varphi(t-1)$. If a required polynomial $S_m(t)$ exists, then

$$\nabla S_m(t) = t^m, \quad (4.36)$$

because of $S_m(n) - S_m(n-1) = n^m$ for all $n \in \mathbb{N}$. Conversely, if we find $S_m(t) \in \mathbb{Q}[t]$ that solves equation (4.36) and has $S_m(0) = 0$, then equality (4.34) is automatically satisfied, because

$$S_m(n) = n^m + S_m(n-1) = n^m + (n-1)^m + S_m(n-2) = \cdots = n^m + (n-1)^m + \cdots + 1^m + 0^m.$$

Thus, we have to solve the equation (4.36) in $S_m \in \mathbb{Q}[t]$. If ∇ were invertible, we could do this at once by applying ∇^{-1} to both sides. However, the power series $1 - e^{-x}$ is not invertible in $\mathbb{Q}[[x]]$, because it has zero constant term. To avoid this problem, write it as $\frac{1-e^{-x}}{x} \cdot x$, where the first factor gets the unit constant term and becomes invertible. The inverse series to the first factor,

$$\text{td}(x) \stackrel{\text{def}}{=} \frac{x}{1 - e^{-x}} \in \mathbb{Q}[[x]],$$

is called *Todd's series*. Substituting $x = D$ in the equality $\text{td}(x) \cdot (1 - e^{-x}) = x$ leads to $\text{td}(D) \circ \nabla = D$. Thus, if we apply $\text{td}(D)$ to both sides of (4.36), we get

$$DS_m(t) = \text{td}(D)t^m.$$

In other words, the derivative $S'_m(t)$ is equal to the m th Appell polynomial $\text{td}_m(t)$ of Todd's series. Since S_m has zero constant term, $S_m(t) = \int \text{td}_m(t) dt$. To make this answer more precise, let us write Todd's series in "exponential form," that is, introduce $a_i \in \mathbb{Q}$ such that

$$\text{td}(x) = \sum_{k \geq 0} \frac{a_k}{k!} x^k. \quad (4.37)$$

Then

$$S_m(t) = \int \left(\sum_{k=0}^m \frac{a_k}{k!} D^k t^m \right) dt = \int \left(\sum_{k=0}^m \binom{m}{k} a_k t^{m-k} \right) dt = \sum_{k=0}^m \binom{m}{k} \frac{a_k t^{m-k+1}}{m-k+1}.$$

So,

$$S_m(t) = \frac{1}{m+1} \times \left(\binom{m+1}{1} a_m t + \binom{m+1}{2} a_{m-1} t^2 + \cdots + \binom{m+1}{m} a_1 t^m + \binom{m+1}{m+1} a_0 t^{m+1} \right).$$

This formula is often symbolically represented as

$$(m+1) \cdot S_m(t) = (a \downarrow + t)^{m+1} - a_{m+1},$$

where the arrow in $a \downarrow$ indicates that a^k is to be replaced by a_k in the expansion of the binomial $(a+t)^{m+1}$. The coefficients a_k of Todd's series (4.37) can be found one by one from the relation

$$\left(1 + a_1x + \frac{a_2}{2}x^2 + \frac{a_3}{6}x^3 + \frac{a_4}{24}x^4 + \cdots\right) \cdot \left(1 - \frac{1}{2}x + \frac{1}{6}x^2 - \frac{1}{24}x^3 + \frac{1}{120}x^4 - \cdots\right) = 1,$$

which says that $\text{td}(x) \cdot (1 - e^{-x})/x = 1$. For example, $a_1 = \frac{1}{2}$, $a_2 = \frac{1}{6}$, $a_3 = 0$, $a_4 = -\frac{1}{30}$, and

$$3S_2(t) = 3a_2t + 3a_1t^2 + t^3 = \frac{1}{2}t + \frac{3}{2}t^2 + t^3,$$

$$4S_3(t) = 4a_3t + 6a_2t^2 + 4a_1t^3 + t^4 = t^2 + 2t^3 + t^4,$$

in agreement with (4.35).

Exercise 4.12 Compute the first dozen of the a_k , continue the list (4.35) up to $S_{10}(n)$, and evaluate⁸ $S_{10}(1000)$.

4.4.2 Bernoulli Numbers

Todd's series got its name in the middle of the twentieth century when it appeared in algebraic topology. In the seventeenth and eighteenth centuries, Jacob Bernoulli and Leonhard Euler, who were the first developers of the subject, preferred to use the power series

$$\text{td}(-x) = \frac{x}{e^x - 1} = \sum_{k \geq 0} \frac{B_k}{k!} x^k,$$

whose coefficients B_k came to be called the *Bernoulli numbers*. Since we have

$$\text{td}(x) - \text{td}(-x) = \frac{x}{1 - e^{-x}} + \frac{x}{1 - e^x} = x \cdot \frac{2 - e^x - e^{-x}}{(1 - e^{-x}) \cdot (1 - e^x)} = x, \quad (4.38)$$

⁸Jacob Bernoulli (1654–1705) did this job in about seven minutes having just pen and paper, as he wrote (not without some pride) in his *Ars Conjectandi*, published posthumously in 1713 (see [Be]).

all but the first Bernoulli numbers coincide with the coefficients a_k used above, i.e., $B_k = a_k$ for all $k \neq 1$, whereas $B_1 = -a_1 = -\frac{1}{2}$. Moreover, it follows from (4.38) that the odd part of Todd's series is exhausted by the linear term. This forces $B_{2k+1} = 0$ for all $k \geq 1$. An extensive literature is devoted to the Bernoulli numbers⁹ B_{2k} . However, despite many beautiful theorems about them, not much is known about the *explicit* dependence of B_{2k} on k .

Exercise 4.13 Prove the recurrence relation $(n+1)B_n = -\sum_{k=0}^{n-1} \binom{n+1}{k} \cdot B_k$.

4.5 Fractional Power Series

4.5.1 Puiseux Series

A Laurent series in the variable $x^{1/q}$, that is, a formal sum of the type

$$f(x) = \sum_{k \geq m} a_k x^{k/q}, \quad a_k \in \mathbb{k}, \quad k \in \mathbb{Z},$$

is called a *Puiseux series* in the variable x with coefficients in \mathbb{k} . In other words, a Puiseux series is a *fractional power series* whose exponents are bounded from below and admit a common denominator.

Exercise 4.14 Convince yourself that the Puiseux series form a field.

Theorem 4.3 *For an algebraically closed field \mathbb{k} of zero characteristic, the field of Puiseux series in x with coefficients in \mathbb{k} is algebraically closed too.*

Less formally, Theorem 4.3 says that the roots y_1, y_2, \dots, y_n of a polynomial

$$a_n(x)y^n + a_{n-1}(x)y^{n-1} + \dots + a_1(x)y + a_0(x)$$

whose coefficients are Puiseux series in x can be expanded as a Puiseux series in x . In particular, given a polynomial $f(x, y) \in \mathbb{k}[x, y]$, the equation $f(x, y) = 0$, considered as a polynomial equation in y with coefficients in $\mathbb{k}[x]$, can be completely solved in Puiseux series $y(x)$. In other words, the implicit algebraic functions over an algebraically closed field \mathbb{k} are exhausted by the Puiseux series. We give two proofs of Theorem 4.3. The first, short and conceptual, goes back to van der Waerden and Hensel. The second, which allows us to expand implicit algebraic functions in Puiseux series effectively, was the original discovery of Newton.

⁹To begin with, I recommend Chapter 15 of the book *A Classical Introduction to Modern Number Theory*, by K. Ireland and M. Rosen [IR] and Section V.8 in the book *Number Theory* by Z. I. Borevich and I. R. Shafarevich [BS]. At <http://www.bernoulli.org/> you may find a fast computer program that evaluates B_{2k} as rational simplified fractions.

Lemma 4.4 (Hensel's Lemma) *Let $G(t, x) \in \mathbb{K}[[t]][x]$ be a monic polynomial in the variable x with coefficients in $\mathbb{K}[[t]]$, where \mathbb{K} is an arbitrary field. Assume that for $t = 0$, the polynomial $G(0, x) \in \mathbb{K}[x]$ is a product of two coprime monic polynomials of positive degree: $G(0, x) = a(x) \cdot b(x)$. Then in $\mathbb{K}[[t]][x]$, the polynomial $G(t, x)$ is also a product of two coprime monic polynomials, $G(t, x) = A(t, x) \cdot B(t, x)$, such that the degrees of A, B in x are equal to those of a, b , and $A(0, x) = a(x)$, $B(0, x) = b(x)$.*

Proof Write $G(t, x)$, $A(t, x)$, and $B(t, x)$ as power series in t with coefficients in $\mathbb{K}[x]$:

$$G(t, x) = g_0(x) + g_1(x)t + g_2(x)t^2 + \cdots,$$

$$A(t, x) = a_0(x) + a_1(x)t + a_2(x)t^2 + \cdots,$$

$$B(t, x) = b_0(x) + b_1(x)t + b_2(x)t^2 + \cdots.$$

Comparing coefficients of t^k in the equality $G(t, x) = A(t, x) \cdot B(t, x)$ leads to a system of equations

$$a_0(x) b_0(x) = g_0(x) \quad (\text{for } k = 0),$$

$$a_0(x) b_k(x) + b_0(x) a_k(x) = g_k(x) - \sum_{i=1}^{k-1} a_i(x) b_{k-i}(x) \quad (\text{for } k \geq 1). \quad (4.39)$$

We are given coprime monic polynomials $a_0(x) = a(x)$, $b_0(x) = b(x)$ satisfying the first equation. The polynomials a_k, b_k of degrees $\deg a_k < \deg a$ and $\deg b_k < \deg b$ are uniquely determined by equation (4.39) as soon as we know all the previous a_i, b_i and know that $\deg a_i < \deg a$ and $\deg b_i < \deg b$ for all $i < k$. Indeed, since $G(t, x)$ is monic as a polynomial in x , for all k we have the inequalities $\deg g_k < \deg g_0$. Therefore, the degree of the right-hand side in (4.39) is strictly less than $\deg a_0 \cdot \deg b_0$. Thus, b_k is the unique polynomial of degree less than $\deg b_0$ whose residue modulo b_0 represents the quotient of the right-hand side by a_0 modulo¹⁰ b_0 . The residue of a_k modulo a_0 plays a similar role. Hence, A and B exist and have the required degrees. To verify that A and B are coprime in $\mathbb{K}[[t]][x]$, we have to construct two series of polynomials $p_i, q_i \in \mathbb{K}[x]$ of degrees bounded above such that the power series $P(t, x) = p_0(x) + p_1(x)t + p_2(x)t^2 + \cdots$, $Q(t, x) = q_0(x) + q_1(x)t + q_2(x)t^2 + \cdots$ satisfy the equality $AP + BQ = 1$. Comparing coefficients of t^k leads, as above, to a system of equations

$$a_0 p_0 + b_0 q_0 = 1 \quad (\text{for } k = 0),$$

$$a_0 p_k + b_0 q_k = - \sum_{i=1}^{k-1} (a_i p_{k-i} + b_i q_{k-i}) \quad (\text{for } k \geq 1).$$

¹⁰Compare with the proof of Proposition 4.1 on p. 76.

Since $a_0 = a$ and $b_0 = b$ are coprime and the inequalities $\deg a_i < \deg a_0$, $\deg b_i < \deg b_0$ hold for all $i > 0$, this system uniquely determines polynomials p_i , q_i of degrees less than $\deg a_0$, $\deg b_0$ respectively. \square

Lemma 4.5 *Let \mathbb{k} be an algebraically closed field of zero characteristic. Then for every polynomial*

$$F(t, x) = a_n(t)x^n + a_{n-1}(t)x^{n-1} + \cdots + a_0(x) \in \mathbb{k}((t))[x],$$

there exist $m \in \mathbb{N}$ and a Laurent series $\vartheta(t) \in \mathbb{k}((t))$ such that $F(t^m, \vartheta(t)) = 0$ in $\mathbb{k}((t))$. In other words, each polynomial with coefficients in $\mathbb{k}((t))$ acquires a root in $\mathbb{k}((t^{1/m}))$ for appropriate $m \in \mathbb{N}$.

Proof Without loss of generality, we may assume that the coefficients of F lie in $\mathbb{k}[[t]]$, that the leading coefficient is $a_n = 1$, and that the next coefficient is $a_{n-1} = 0$. The first is achieved via multiplication of F by an appropriate power of t , the second by multiplication of F by a_n^{n-1} and renaming $a_n x$ by x , and the third by changing the variable¹¹ x to $x - a_{n-1}/n$.

Exercise 4.15 For each of the three manipulations, verify that if the lemma holds for the modified polynomial, then it holds for the original one.

If F is factorized in $\mathbb{k}[[t]][x]$ as $F = GH$, where $0 < \deg G < \deg F$, we can apply induction on $\deg F$ and find m and ϑ for G instead of F . Now assume that F is irreducible. Then by Hensel's lemma, the polynomial $F(0, x) \in \mathbb{k}[x]$ cannot be decomposed in $\mathbb{k}[x]$ into a product of two coprime polynomials of positive degree. Over the algebraically closed field \mathbb{k} , this forces $F(0, x)$ to have a root of multiplicity $\deg F$. Therefore, $F(0, x) = (x - \alpha)^n$ for some $\alpha \in \mathbb{k}$. If $\alpha \neq 0$, the polynomial $(x - \alpha)^n$ contains a nonzero term¹² $n\alpha x^{n-1}$ of degree $(n - 1)$. This contradicts our assumption on F . Hence, $F(0, x) = x^n$. This means that every series $a_m(t)$ has a zero constant term. If each of the a_i is the zero series, then $F(t, x) = x^n$ has a root $\vartheta(t) = 0$. Assume that not all the $a_i(t)$ are zero. We claim that for appropriate $p, q \in \mathbb{N}$, the substitution $t \leftarrow t^q$, $x \leftarrow t^p x$, transforms the polynomial F into the polynomial $t^{np} \cdot H$, where H , as a polynomial in x , is monic and has no term of degree $n - 1$, and at least one coefficient of H is a series with nonzero constant term. This forces H to be reducible, and we will be able to apply induction.

The first two constraints on H are automatically satisfied under the substitution $t \leftarrow t^q$, $x \leftarrow t^p x$. With respect to the third, write each nonzero coefficient a_m in F as

$$a_m(t) = \alpha_{\mu_m} t^{\mu_m} + \text{terms of higher degree in } t,$$

where $\alpha_{\mu_m} \neq 0$ is the lowest nonzero coefficient. We take q equal to the common denominator of all fractions $\mu_m/(n - m)$. Then rewrite all these fractions as p_m/q

¹¹Here we use that $n = 1 + \cdots + 1 \neq 0$ in \mathbb{k} .

¹²Here we use again that $\text{char } \mathbb{k} = 0$.

and put $p = \min(p_m)$. Therefore, for each m , we get the inequality $q\mu_m \geq p(n-m)$, which becomes an explicit equality for some m . The polynomial

$$\begin{aligned} G(t, x) &= F(t^q, t^p x) = t^{pn} x^n + \sum_{m=0}^{n-2} a_m(t^q) t^{pm} x^m \\ &= t^{pn} x^n + \sum_{m=0}^{n-2} t^{pm} (\alpha_{\mu_m} t^{q\mu_m} + \text{terms of higher degree in } t) \cdot x^m \\ &= t^{pn} \left(x^n + \sum_{m=0}^{n-2} t^{q\mu_m - p(n-m)} (\alpha_{\mu_m} + \text{terms of higher degree in } t) \cdot x^m \right) \end{aligned}$$

is divisible by t^{pn} in $\mathbb{k}[[t]][x]$. Write $H(t, x) = \sum h_m(t) \cdot x^m$ for the quotient $G(t, x)/t^{pn}$. Then the coefficient h_m in H has nonzero constant term for those m for which the equality $q\mu_m = p(n-m)$ is achieved. Hence, the polynomial $H(t, x)$ is reducible, and therefore, there exist $d \in \mathbb{N}$ and $\tau(t) \in \mathbb{k}((t))$ such that $H(t^d, \tau(t)) = 0$ in $\mathbb{k}((t))$. Then for $m = qd$ and $\vartheta(t) = t^p \tau(t)$, we have $F(t^m, \vartheta(t)) = F(t^{qd}, t^p \tau(t)) = t^{pn} H(t^d, \tau(t)) = 0$. \square

Proof (of Theorem 4.3) Given a polynomial $f(x) = a_0(t) + a_1(t)x + \cdots + a_n(t)x^n$ whose coefficients $a_i(t)$ are Puiseux series, write m for the common denominator of all exponents in all series a_i and put $t = u^m$. Then $a_i(t) = a_i(u^m) \in \mathbb{k}((u))$, and by Lemma 4.5, the polynomial f acquires a root in the field $\mathbb{k}((s))$ after the appropriate parameter change $u = s^q$. Returning to the initial parameter $t = s^{qm}$, we get a root of f in the field of Laurent series in $t^{1/qm}$, which is a subfield in the field of Puiseux series. \square

Example 4.9 (Counterexample to Theorem 4.3 in Positive Characteristic) The proof of Lemma 4.5 essentially uses the assumption $\text{char } \mathbb{k} = 0$, without which both Lemma 4.5 and Theorem 4.3 fail. To demonstrate this, put $\mathbb{k} = \mathbb{F}_p$ and consider the equation $x^p - x = t^{-1}$ over the field $\mathbb{F}_p((t))$. Let us try to equip the power series $x(t) = c_1 t^{\lambda_1} + c_2 t^{\lambda_2} + \cdots$ with rational $\lambda_1 < \lambda_2 < \cdots$ and nonzero $c_i \in \mathbb{F}_p$ to solve the equation. Since $c^p = c$ for all $c \in \mathbb{F}_p$, the substitution of $x = x(t)$ into $tx^p - tx = 1$ leads to

$$-c_1 t^{\lambda_1+1} + c_2 t^{\lambda_2+1} - c_1 t^{p\lambda_1+1} + c_3 t^{\lambda_3+1} - c_2 t^{p\lambda_2+1} + \text{higher powers of } t = 1.$$

The lowest term $c_1 t^{\lambda_1+1}$ can be canceled only by the 1 on the right-hand side. Hence, $\lambda_1 = -1$ and $c_1 = -1$. The next two terms have to cancel each other. Hence, $\lambda_2 = -p^{-1}$ and $c_2 = c_1$. The next two terms also should kill each other. Therefore, $\lambda_3 = -p^{-2}$ and $c_3 = c_2$, etc. We conclude that

$$x(t) = -t^{-1} - t^{-1/p} - t^{-1/p^2} - t^{-1/p^3} - \cdots = -\sum_{k \geq 0} t^{-p^{-k}}.$$

This fractional power series is not a Puiseux series, because its exponents do not have a common denominator.

4.5.2 Newton's Method

Consider the monic polynomial equation

$$F(t, x) = x^n + a_{n-1}(t)x^{n-1} + \cdots + a_0(t) = 0 \quad (4.40)$$

with coefficients $a_i(t) \in \mathbb{k}[[t]]$ such that $a_0(0) = 0$, which means that the initial polynomial $F(0, x) \in \mathbb{k}[x]$ has a zero root. Newton's method allows us to compute all solutions $x(t)$ of (4.40) such that $x(0) = 0$. If $\xi \in \mathbb{k}$ is a nonzero root of the initial polynomial $F(0, x)$, then to find all solutions $x(t)$ starting with $x(0) = \xi$ by Newton's method, one should first shift the variable by the substitution $x \leftarrow x + \xi$. An arbitrary polynomial equation with coefficients in the field of Puiseux series can be reduced to (4.40) by the standard manipulations used in the proof of Lemma 4.5.

Essentially, Newton's method visualizes the main step in the proof of Lemma 4.5. Let us depict by an integer point (p, q) in the coordinate plane each monomial¹³ $x^p t^q$ appearing in $F(t, x)$ with nonzero coefficient. The convex hull of all these points is called the *Newton polygon* of the polynomial $F(t, x)$. The broken line formed by all the edges of the Newton polygon visible from the origin is called the *Newton diagram* of F . Since F is monic and $a_0(0) = 0$, the Newton diagram does not contain the origin and has its endpoints on the coordinate axes. All integer points (m, μ_m) of the Newton diagram depict the terms of lowest degree in t of some of the coefficients¹⁴

$$a_m(t) = \alpha_{\mu_m} t^{\mu_m} + \text{higher powers of } t$$

in F . For example, Fig. 4.1 shows the Newton polygon of the polynomial

$$(-t^3 + t^4) - 2t^2 x - tx^2 + 2tx^4 + x^5. \quad (4.41)$$

Its Newton diagram consists of two edges perpendicular to the vectors $(1, 1)$ and $(1, 3)$.

We are going to compute successive positive rational numbers $\varepsilon_1, \varepsilon_2, \dots$ and nonzero elements c_1, c_2, \dots of \mathbb{k} such that the power series

$$x(t) = c_1 t^{\varepsilon_1} + c_2 t^{\varepsilon_1 + \varepsilon_2} + c_3 t^{\varepsilon_1 + \varepsilon_2 + \varepsilon_3} + \cdots = t^{\varepsilon_1} \left(c_1 + t^{\varepsilon_2} (c_2 + t^{\varepsilon_3} (c_3 + \cdots)) \right) \quad (4.42)$$

extends the zero root of $F(0, x)$ in the field \mathbb{k} to some root of $F(t, x)$ in the field of Puiseux series.

¹³Note that the exponent of x grows along the *horizontal* axis.

¹⁴But not all, in general.

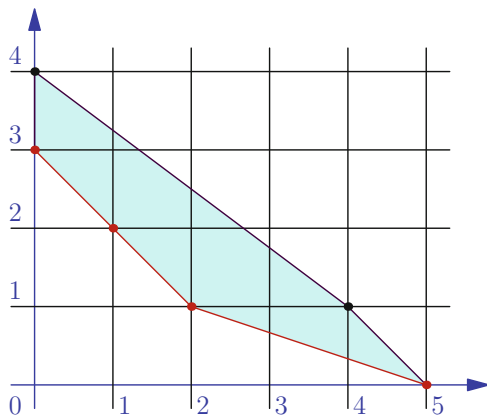


Fig. 4.1 The Newton polygon of $(-t^3 + t^4) - 2t^2x - tx^2 + 2tx^4 + x^5$

When we substitute the series (4.42) for x in $F(t, x)$, the product of the terms of lowest degree in t of the series $x^m(t)$ and $a_m(t)$ is equal to

$$a_{\mu_m} c_1^m t^{m\varepsilon_1 + \mu_m}. \quad (4.43)$$

Several such terms will cancel each other if they have the same degree in t , i.e., the same value of $m\varepsilon_1 + \mu_m$. This happens if and only if the exponents of the monomials (4.43) lie on the same line $p\varepsilon_1 + q = \text{const}$ containing some edge of the Newton diagram. At the first step of Newton's method, we choose some edge Z . Let the integer vector $v_Z = (\delta_1, \delta_2)$ be perpendicular to Z and satisfy $\text{GCD}(\delta_1, \delta_2) = 1$. We put $\varepsilon_1 = \delta_1/\delta_2$, the slope of v_Z . Then we substitute

$$x(t) = c_1 t^{\varepsilon_1} + \text{higher powers of } t$$

for x in F and choose $c_1 \in \mathbb{k}$ such that all monomials (4.43), which have the lowest degree in t , turn out to be canceled in $F(t, x(t))$. These monomials are depicted by the points (p, q) lying on the edge Z . Thus, it is reasonable to collect the monomials in $F(t, x)$ along the lines $\delta_1 p + \delta_2 q = \text{const}$, that is, write F as $F(t, x) = \sum_{i \geq \gamma} f_i(t, x)$, where $\gamma \in \mathbb{N}$ is the value of the linear form $\delta_1 p + \delta_2 q$ on Z , i.e., such that $\varepsilon_1 p + q = \gamma/\delta_2$, and

$$f_i(t, x) = \sum_{\delta_1 p + \delta_2 q = i} \alpha_{p, q} x^p t^q. \quad (4.44)$$

The term of $f_i(t, x(t))$ of lowest degree in t equals $t^{i/\delta_2} f_i(1, c_1)$. Thus, the minimal power t^{γ/δ_2} in $F(t, x(t))$ disappears if and only if c_1 is a root of the polynomial $f_\gamma(1, x) \in \mathbb{K}[x]$. Different roots lead to different Puiseux series (4.42) starting from $c_1 t^{\varepsilon_1}$.

Exercise 4.16 Write λ for the abscissa of the left endpoint of Z . Verify that x^λ divides $f_\gamma(1, x)$ in $\mathbb{K}[x]$.

At the second step of Newton's method, we substitute $t^{\varepsilon_1}(c_1 + x)$ for x in the polynomial $F(t, x)$. The resulting polynomial $G(t, x) = F(t, t^{\varepsilon_1}(c_1 + x))$ is divisible by t^{γ/δ_2} . We write $F_1(t, x)$ for the quotient and repeat the first step with F_1 instead of F . This leads to the next exponent ε_2 , the next coefficient c_2 , and the next polynomial F_2 , etc.

For example, let us find the roots of the polynomial (4.41). The normal vector to the left edge of the Newton diagram in Fig. 4.1 has coordinates $(1, 1)$ and leads to $\varepsilon_1 = 1$. Lying on this edge are the monomials $-t^3$, $-2t^2x$, $-tx^2$ of F . Thus, $\gamma = 3$ and $f_3(1, x) = -1 - 2x - x^2 = -(x + 1)^2$ has just one root $c_1 = -1$. Substituting $t(x - 1)$ for x in (4.41) and canceling the factor t^3 , we get

$$-x^2 + t + t^2(-1 + x)^4(1 + x) = (t + t^2) - 3t^2x + (-1 + 2t^2)x^2 + 2t^2x^3 - 3t^2x^4 + t^2x^5 \quad (4.45)$$

as $F_1(t, x)$. Its Newton polygon is shown in Fig. 4.2.

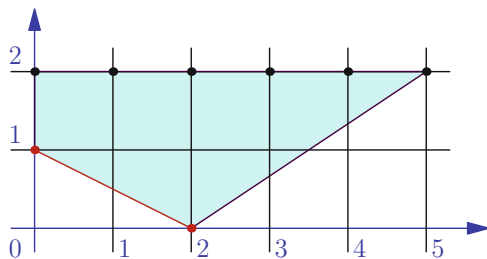


Fig. 4.2 The Newton polygon of $(t + t^2) - 3t^2x + (-1 + 2t^2)x^2 + 2t^2x^3 - 3t^2x^4 + t^2x^5$

The Newton diagram consists of just one edge with normal vector $(1, 2)$. So $\varepsilon_2 = 1/2$. The lowest term of (4.44) is $f_2(t, x) = t - x^2$. Thus, c_2 is a root of the polynomial $f_2(1, x) = 1 - x^2$. There are two possibilities: $c_2 = \pm 1$. Let us take $c_2 = 1$ first. After substituting $x \leftarrow t^{1/2}(1 + x)$, the polynomial (4.45) becomes

$$(t - 3t^{3/2} + \dots) + (-2 - 3t^{3/2} + \dots)x + (-1 - 2t^3 + \dots)x^2 + \dots.$$

Here the Newton diagram consists of one edge joining $(0, 1)$ and $(1, 0)$.

Exercise 4.17 Show that carrying out additional steps of Newton's method will not change the Newton diagram.

We conclude that the root we obtain in this way is a power series in $t^{1/2}$. If we write it with indeterminate coefficients and substitute in F , then we get explicit recurrence formulas allowing us to compute the coefficients one by one.

Exercise 4.18 Check that the root corresponding to the choice $c_2 = -1$ in the previous step is also a power series in $t^{1/2}$.

Returning to the first step, consider the segment in the Newton diagram of Fig. 4.1 with endpoints $(2, 1)$ and $(5, 0)$. The normal vector of this edge is $(1, 3)$. Thus, $\varepsilon_1 = 1/3$. The coefficient c_1 is a root of $f_5(1, x)/x^2 = -1 + x^3$. We can choose among the three values $c_1 = 1, \omega, \omega^2$, where $\omega \in \mathbb{K}$ is a primitive cube root of unity. Let us take $c_2 = \omega$. After the substitution $x \leftarrow t^{1/3}(\omega + x)$ in (4.41) and canceling the factor $t^{5/3}$, we get the polynomial

$$\begin{aligned} &(-t^{4/3} + t^{7/3}) + (3\omega + 6t^{2/3})x + (9 + 12\omega^2 t^{2/3})x^2 + (10\omega^2 + 8\omega t^{2/3})x^3 \\ &+ (5\omega + 2t^{2/3})x^4 + x^5. \end{aligned}$$

Its Newton diagram is again one edge joining $(0, 1)$ to $(1, 0)$. Thus, the current root is a power series in $t^{1/3}$. Choosing the two remaining values of c_2 , we arrive at a similar result. Thus, the five roots of the polynomial (4.41) are two power series in $t^{1/2}$, which begin with $-t \pm t^{3/2} + \dots$, and three power series in $t^{1/3}$ with initial terms $t^{1/3}, \omega t^{1/3}, \omega^2 t^{1/3}$.

Let us make some final remarks on the general case. Write $\ell(Z)$ for the length of the *horizontal projection* of the edge Z . It is clear that the denominator of $\varepsilon_1 = \delta_1/\delta_2$ is not greater than $\ell(Z)$. The degree of the polynomial $f_\gamma(1, x)/x^\lambda$, whose root is c_1 , equals the number of segments into which Z is broken by the integer points. Therefore, it is also not greater than $\ell(Z)$. If c_1 is a root of multiplicity d , then $f_\gamma(1, x) = (x - c_1)^d g(x)x^\lambda$, where $g(c_1) \neq 0$, and

$$f_\gamma(1, c_1 + x) = x^d c_1^\lambda g(c_1) + \text{higher powers of } x$$

contains the nonzero term $g(c_1)c_1^\lambda x^d$, depicted by $(d, 0)$. Therefore, the Newton diagram of the next polynomial $F(t, t^{\varepsilon_1}(c_1 + x))/t^{\gamma/\delta_2}$ meets the horizontal axis at $(d, 0)$ or to the left of it. This means that the length of the horizontal projection of any edge of the diagram is at most d , the multiplicity of the root c_1 . In particular, the next exponent after a simple root c_1 has to be an *integer*.

Proposition 4.5 Every output series $x(t)$ of Newton's method applied to the polynomial $F(t, x)$ is a Puiseux series that satisfies the equation¹⁵ $F(t, x(t)) = 0$ in $\mathbb{K}[[t]]$.

Proof Let us show that the exponents of an output series $x(t)$ have a common denominator. It is enough to verify that all ε_i but a finite number are integers. As we

¹⁵Note that this gives another proof of Lemma 4.5.

have just seen, the denominator of ε_{i+1} is at most $\ell(Z_{i+1})$, which is not greater than the multiplicity of the root c_i chosen in the previous step. In turn, this multiplicity is at most $\ell(Z_i)$. We obtain the inequality $\ell(Z_{i+1}) \leq \ell(Z_i)$, which will be an equality only if c_i is a root of multiplicity $\ell(Z_i)$. Since the degree of $f_\gamma(x, 1)/x^\lambda$ is at most $\ell(Z_i)$, such a multiplicity of c_i is possible only for

$$f_{\gamma_i}(x, 1)/x^{\lambda_i} = \alpha \cdot (x - c_i)^{\ell(Z_i)}, \quad \alpha \in \mathbb{K}, \alpha \neq 0.$$

In this case, the horizontal projections of integer points lying on Z_i cover all integers in the range from λ to $\lambda + \ell(Z_i)$. This forces the normal vector of Z to be of the form $n_Z = (\delta, 1)$ for $\delta \in \mathbb{N}$. Hence, $\varepsilon_{i+1} = \delta \in \mathbb{N}$ in this case. We conclude that either $\ell(Z_{i+1}) < \ell(Z_i)$ or ε_{i+1} is an integer. Therefore, all the exponents ε_i after some finite number of iterations will be integers.

Now the equality $F(t, x(t)) = 0$ can be verified easily. After the i th step of Newton's algorithm, we are sure that the degree of the lowest term in the series $F(t, x(t))$ is at least the sum of all the fractions γ/δ_2 appearing in the first i steps. Since we always have $\gamma \geq 1$ and $\delta_2 = 1$ after a finite number of steps, this sum is unbounded from above. \square

Problems for Independent Solution to Chap. 4

Problem 4.1 Compute the antiderivative and the 1000th derivative of the function $x^4/(1+x^2)$.

Problem 4.2 Write the n th coefficients of the following power series as explicit functions of n :

- (a) $(2x^2 - 3x + 1)^{-1}$, (b) $(x^4 + 2x^3 - 7x^2 - 20x - 12)^{-1}$, (c) $\sqrt[3]{1+2x}$,
 (d) $1/\sqrt{1-3x}$, (e) $\cosh(x) \stackrel{\text{def}}{=} (e^x + e^{-x})/2$, (f) $\sinh(x) \stackrel{\text{def}}{=} (e^x - e^{-x})/2$,
 (g) $\cos(x) \stackrel{\text{def}}{=} (e^{ix} + e^{-ix})/2$, (h) $\sin(x) \stackrel{\text{def}}{=} (e^{ix} - e^{-ix})/2i$.

Problem 4.3 Express a_k as an explicit function of k for the following sequences:

- (a) $a_0 = 1, a_1 = -1, a_k = 2a_{k-1} - a_{k-2}$ for all $k \geq 2$,
 (b) $a_0 = 1, a_1 = q, a_k = (1+q)a_{k-1} - qa_{k-2}$ for all $k \geq 2$, where $q \in \mathbb{C}$,
 (c) $a_0 = 0, a_1 = 1, a_2 = 5, a_3 = 14, a_k = 4a_{k-1} - 6a_{k-2} + 4a_{k-3} - a_{k-4}$ for all $k \geq 4$.

Problem 4.4 Let $g(x) = \prod (x - \alpha_i)$, where all α_i are distinct. For a polynomial $f \in \mathbb{K}[x]$ such that $\deg f < \deg g$, prove the following partial fraction expansion¹⁶:

$$f(x)/g(x) = \sum \frac{f(\alpha_i)/g'(\alpha_i)}{(x - \alpha_i)}, \text{ where } g' = \frac{d}{dx}g.$$

¹⁶See Proposition 4.1 on p. 76.

Problem 4.5 (Taylor Expansion) Let \mathbb{k} be a field of zero characteristic. Given a point $a \in \mathbb{k}$ and $n + 1$ values $b_0, b_1, \dots, b_n \in \mathbb{k}$, construct a polynomial $f \in \mathbb{k}[x]$ such that $\deg f \leq n$, $f(a) = b_0$, $(d/dx)^i f(a) = b_i$ for all $i = 1, \dots, n$, and prove that such a polynomial is unique.

Problem 4.6 Show that all coefficients of the power series $\tan(x) \stackrel{\text{def}}{=} \sin(x)/\cos(x)$ are positive.

Problem 4.7 Show that $e^x \in \mathbb{Q}[[x]] \setminus \mathbb{Q}(x)$.

Problem 4.8 Find an $f \in \mathbb{Q}[[x]] \setminus \mathbb{Q}(x)$ whose nonzero coefficients all are equal to 1.

Problem 4.9 Write $p_m(n)$ for the total number of Young diagrams consisting of n cells and at most m rows. Also put $p_m(0) \stackrel{\text{def}}{=} 1$. Express $p_m(n)$ in terms of $p_{m-1}(n)$ and $p_m(n-m)$. Show that the generating series $P_m(x) = \sum_{n \geq 0} p_m(n) x^n \in \mathbb{Q}[[x]]$ is a rational function.

Problem 4.10 (Euler's Pentagonal Theorem) Write $p(n)$ for the number of Young diagrams of weight¹⁷ n and $\hat{p}_{\text{even}}(n)$ (respectively $\hat{p}_{\text{odd}}(n)$) for the number of weight- n Young diagrams consisting of an even (respectively odd) number of rows of distinct lengths. Put $p(0) \stackrel{\text{def}}{=} 1$ and consider the generating series $P(x) = \sum_{n \geq 0} p(n) x^n \in \mathbb{Q}[[x]]$. Show that

$$(a) P(x) = \prod_{k \geq 1} (1 - x^k)^{-1}, \quad (b) \frac{1}{P(x)} = 1 + \sum_{n \geq 1} (\hat{p}_{\text{even}}(n) - \hat{p}_{\text{odd}}(n)) \cdot x^n,$$

$$(c) p(n) = \sum_{k \geq 1} (-1)^{k+1} \left(p(n - (3k^2 - k)/2) + p(n - (3k^2 + k)/2) \right) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) - \dots,$$

and evaluate $p(10)$.

Problem 4.11 A triangulation of a convex n -gon by some of its diagonals is *admissible* if the diagonals do not intersect each other anywhere except at the vertices of the n -gon. For example, the 4-gon, 5-gon, and 6-gon admit 2, 5, and 12 such triangulations. How many admissible triangulations are there for an arbitrary n ?

Problem 4.12 Write i_m for the total number of monic irreducible polynomials of degree¹⁸ m in $\mathbb{F}_p[x]$. Prove that $(1 - px)^{-1} = \prod_{m \in \mathbb{N}} (1 - x^m)^{-i_m}$ in $\mathbb{Q}[[t]]$.

Problem 4.13 Express the differentiation operator $\frac{d}{dt} : \mathbb{Q}[t] \rightarrow \mathbb{Q}[t]$, $f \mapsto f'$, as a power series in the difference operator $\nabla : \mathbb{Q}[t] \rightarrow \mathbb{Q}[t]$, $f(t) \mapsto f(t) - f(t-1)$, i.e., find a power series $\Psi \in \mathbb{Q}[[x]]$ without a constant term such that $\Psi(\nabla) = \frac{d}{dt}$.

Problem 4.14 Verify that the polynomials

$$\gamma_0 \equiv 1 \quad \text{and} \quad \gamma_k(t) \stackrel{\text{def}}{=} \binom{t+k}{k} = \frac{1}{k!} (t+1)(t+2) \cdots (t+k) \quad \text{for } k > 0 \quad (4.46)$$

satisfy the relations $\nabla^n \gamma_k = \gamma_{k-n}$ and use this to prove that every polynomial $f \in \mathbb{Q}[t]$ can be linearly expressed through polynomials (4.46) by the formula

¹⁷That is, consisting of n cells; the number $p(n)$ is also called the n th *partition number*; see Example 1.3 on p. 6.

¹⁸Compare with Problem 3.12 on p. 67.

$f = \sum_k \nabla^k f(-1) \cdot \gamma_k$. Also show that the coefficients $c_k \in \mathbb{Q}$ of every linear expression $f = \sum_k c_k \cdot \gamma_k$ have to be $c_k = \nabla^k f(-1)$.

Problem 4.15 Write $T_\alpha \stackrel{\text{def}}{=} e^{-\alpha D} : f(x) \mapsto f(x - \alpha)$ for the shift-by- α operator¹⁹ and put $T = T_1$. Prove that the following properties of the linear map²⁰ $F : \mathbb{Q}[t] \rightarrow \mathbb{Q}[t]$ are equivalent:

- (1) $F \circ \nabla = \nabla \circ F$, (2) $F \circ T = T \circ F$, (3) $\forall \alpha \in \mathbb{Q}, F \circ T_\alpha = T_\alpha \circ F$,
 (4) $\exists \Phi \in \mathbb{Q}[[x]] : F = \Phi(D)$, (5) $\exists \Psi \in \mathbb{Q}[[x]] : F = \Psi(\nabla)$.

Problem 4.16 Prove that the Bernoulli numbers B_{2k} are positive for odd $k \geq 1$ and negative for even $k \geq 2$.

Problem 4.17 Write the first three nonzero terms of the Puiseux expansion over \mathbb{C} for all roots $x(t)$ of the following polynomials:

- (a) $(t^7 + t^6) - t^3 x + t x^2 - x^3$,
 (b) $t^3 + (-t + t^2)x + x^3$,
 (c) $t^4 - t^3 x + 3t^2 x^3 - 3t x^5 + x^7$,
 (d) $(t^2 + 4t^3 + 6t^4) - 4t^4 x + (-2t - 4t^2 - 2t^3)x^2 + x^4$,
 (e) $2t^5 - t^3 x + 2t^2 x^2 - t x^3 + 2x^5$.

¹⁹Compare with Example 4.7 on p. 89.

²⁰The map $F : \mathbb{Q}[t] \rightarrow \mathbb{Q}[t]$ is *linear* if for all $\alpha, \beta \in \mathbb{Q}$ and all $f, g \in \mathbb{Q}[t]$, the equality $F(\alpha \cdot f + \beta \cdot g) = \alpha F(f) + \beta F(g)$ holds. For example, all the maps $D = \frac{d}{dt}$, D^k , $\Phi(D)$ for all $\Phi \in \mathbb{Q}[[x]]$, ∇ , ∇^k , and $\Phi(\nabla)$ are linear.

Chapter 5

Ideals, Quotient Rings, and Factorization

In this section we continue to use the notation of Chaps. 3 and 4 and write K for an arbitrary commutative ring with unit and \mathbb{k} for an arbitrary field.

5.1 Ideals

5.1.1 Definition and Examples

A subring I in a commutative ring K is called an *ideal* if for every $a \in I$ and $f \in K$, we have $fa \in I$. We have seen in Sect. 2.6.4 that the kernel of a ring homomorphism $\varphi : K \rightarrow L$ is an ideal in K . For every $a \in K$, all multiplies of a form an ideal

$$(a) \stackrel{\text{def}}{=} \{fa \mid f \in K\} \quad (5.1)$$

called the *principal ideal* generated by a . We used principal ideals in the constructions of the residue rings $\mathbb{Z}/(n)$ and $\mathbb{k}[x]/(f)$, where the principal ideals $(n) \subset \mathbb{Z}$ and $(f) \in \mathbb{k}[x]$ were the kernels of the quotient homomorphisms $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n)$, $m \mapsto [m]_n$, and $\mathbb{k}[x] \twoheadrightarrow \mathbb{k}[x]/(f)$, $g \mapsto [g]_f$. Every commutative ring K with unit has the *trivial* ideals $(0) = \{0\}$ and $(1) = K$.

Exercise 5.1 Prove that for every commutative ring K with unit, the following properties of an ideal $I \subset K$ are equivalent: **(a)** I contains an invertible element of K , **(b)** $1 \in I$, **(c)** $I = K$.

Proposition 5.1 A commutative ring K with unit is a field if and only if there are no nontrivial ideals in K .

Proof An ideal in a field is trivial by Exercise 5.1. Conversely, if a nonzero ideal coincides with K , then $(b) = K$ for every $b \neq 0$. Hence, $1 = sb$ for some $s \in K$. Thus, all $b \neq 0$ are invertible. \square

5.1.2 Noetherian Rings

Every subset $M \subset K$ generates an ideal $(M) \subset K$ formed by all finite sums $b_1a_1 + b_2a_2 + \cdots + b_ma_m$, where $a_1, a_2, \dots, a_m \in M$, $b_1, b_2, \dots, b_m \in K$, $m \in \mathbb{N}$.

Exercise 5.2 Verify that $(M) \subset K$ is an ideal.

Every ideal $I \subset K$ is generated by some subset $M \subset K$, e.g., by $M = I$. An ideal $I \subset M$ is said to be *finitely generated* if it admits a finite set of generators, that is, if it can be written as

$$I = (a_1, a_2, \dots, a_k) = \{b_1a_1 + b_2a_2 + \cdots + b_ka_k \mid b_i \in K\}$$

for some $a_1, a_2, \dots, a_k \in I$. We met finitely generated ideals when we constructed the GCD in the rings \mathbb{Z} and $\mathbb{k}[x]$.

Lemma 5.1 *The following properties of a commutative ring K are equivalent:*

- (1) *Every subset $M \subset K$ contains some finite collection of elements $a_1, a_2, \dots, a_k \in M$ such that $(M) = (a_1, a_2, \dots, a_k)$.*
- (2) *Every ideal $I \subset K$ is finitely generated.*
- (3) *For every infinite chain of increasing ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ in K , there exists $n \in \mathbb{N}$ such that $I_v = I_n$ for all $v \geq n$.*

Proof Clearly, (1) \Rightarrow (2). To deduce (3) from (2), write $I = \bigcup I_v$ for the union of all ideals in the chain. Then I is an ideal as well. By (2), I is generated by some finite set of its elements. All these elements belong to some I_n . Therefore, $I_n = I = I_v$ for all $v \geq n$. To deduce (1) from (3), we construct inductively a chain of strictly increasing ideals $I_n = (a_1, a_2, \dots, a_n)$ starting from an arbitrary $a_1 \in M$. While $I_k \neq (M)$, we choose any element $a_{k+1} \in M \setminus I_k$ and put $I_{k+1} = (a_{k+1} \cup I_k)$. Since $I_k \subsetneq I_{k+1}$ in each step, by (3) this procedure has to stop after a finite number of steps. At that moment, we obtain $I_m = (a_1, a_2, \dots, a_m) = (M)$. \square

Definition 5.1 A commutative ring K is said to be *Noetherian* if it satisfies the conditions from Lemma 5.1. Note that every field is Noetherian.

Theorem 5.1 (Hilbert's Basis Theorem) *For every Noetherian commutative ring K , the polynomial ring $K[x]$ is Noetherian as well.*

Proof Consider an arbitrary ideal $I \subset K[x]$ and write $L_d \subset K$ for the set of leading coefficients of all polynomials of degree $\leq d$ in I including the zero polynomial. Also write $L_\infty = \bigcup_d L_d$ for the set of all leading coefficients of all polynomials in I .

Exercise 5.3 Verify that all of the L_d and L_∞ are ideals in K .

Since K is Noetherian, the ideals L_d and L_∞ are finitely generated. For all d (including $d = \infty$), write $f_1^{(d)}, f_2^{(d)}, \dots, f_{m_d}^{(d)} \in K[x]$ for those polynomials whose leading coefficients span the ideal $L_d \subset K$. Let $D = \max \deg f_i^{(\infty)}$. We claim that the polynomials $f_i^{(\infty)}$ and $f_j^{(d)}$ for $d < D$ generate I . Let us show first that each polynomial

$g \in I$ is congruent modulo $f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{m_\infty}^{(\infty)}$ to some polynomial of degree less than D . Since the leading coefficient of g lies in L_∞ , it can be written as $\sum \lambda_i a_i$, where $\lambda_i \in K$ and a_i is the leading coefficient of $f_i^{(\infty)}$. As long as $\deg g \geq D$, all differences $m_i = \deg g - \deg f_i^{(\infty)}$ are nonnegative, and we can form the polynomial $h = g - \sum \lambda_i \cdot f_i^{(\infty)}(x) \cdot x_i^{m_i}$, which is congruent to g modulo I and has $\deg h < \deg g$. We replace g by h and repeat the procedure while $\deg h \geq D$. When we come to a polynomial $h \equiv g \pmod{I}$ such that $\deg h < D$, the leading coefficient of h falls into some L_d with $d < D$, and we can cancel the leading terms of h by subtracting appropriate combinations of polynomials $f_j^{(d)}$ for $0 \leq d < D$ until we get $h = 0$. \square

Corollary 5.1 *For every Noetherian commutative ring K , the ring $K[x_1, x_2, \dots, x_n]$ is Noetherian.* \square

Exercise 5.4 Show that the ring $K[[x_1, x_2, \dots, x_n]]$ is Noetherian for every Noetherian commutative ring K .

Corollary 5.2 *Every infinite system of polynomial equations with coefficients in a Noetherian ring K is equivalent to some finite subsystem.*

Proof Since $K[x_1, x_2, \dots, x_n]$ is Noetherian, among the right-hand sides of a polynomial equation system

$$f_v(x_1, x_2, \dots, x_n) = 0$$

there is some finite collection f_1, f_2, \dots, f_m that generates the same ideal as all the f_v . This means that every f_v is equal to $g_1 f_1 + g_2 f_2 + \dots + g_m f_m$ for some $g_i \in K[x_1, x_2, \dots, x_n]$. Hence, every equation $f_v = 0$ follows from $f_1 = f_2 = \dots = f_m = 0$. \square

Example 5.1 (Non-Noetherian Rings) Consider a countably infinite set of variables x_i numbered by $i \in \mathbb{N}$ and define the polynomial ring $\mathbb{Q}[x_1, x_2, x_3, \dots]$ in these variables to be the set of all finite sums of finite monomials $x_{v_1}^{m_1} x_{v_2}^{m_2} \dots x_{v_s}^{m_s}$ multiplied by arbitrary rational coefficients. The ideal I spanned by the set of all variables consists of all polynomials without a constant term. It coincides with the union of strictly increasing ideals $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset (x_1, x_2, x_3, x_4) \subset \dots$, forming an infinite tower.

Exercise 5.5 Verify that $(x_1, x_2, \dots, x_n) \subsetneq (x_1, x_2, \dots, x_{n+1})$.

Thus, the ideal I is not finitely generated, and the ring $\mathbb{Q}[x_1, x_2, x_3, \dots]$ is not Noetherian. The less artificial rings $\mathcal{C}(\mathbb{R})$ and $\mathcal{C}^\infty(\mathbb{R})$ of all continuous and all infinitely differentiable functions $f: \mathbb{R} \rightarrow \mathbb{R}$ are also not Noetherian.

Exercise 5.6 Write $I_k \subset \mathcal{C}^\infty(\mathbb{R})$ for the set of all functions vanishing on $\mathbb{Z} \cap [-k, k]$. Verify that $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$ form an infinite chain of strictly increasing ideals in $\mathcal{C}^\infty(\mathbb{R})$.

Caution 5.1 A subring of a Noetherian ring is not necessarily Noetherian. For example, the ring of formal power series $\mathbb{C}[[z]]$ is Noetherian by [Exercise 5.4](#), whereas the subring formed by all analytic functions¹ $\mathbb{C} \rightarrow \mathbb{C}$ is not.

Exercise 5.7 Verify this by arguing as in [Exercise 5.6](#).

5.2 Quotient Rings

5.2.1 Factorization Homomorphism

Let a commutative ring K be equipped with an equivalence relation \sim that decomposes K into equivalence classes. Write X for the set of these classes and consider the quotient map sending an element $a \in K$ to its equivalence class $[a] \in X$:

$$\pi : K \twoheadrightarrow X, \quad a \mapsto [a]. \quad (5.2)$$

Let us ascertain whether X admits the structure of a commutative ring such that the map (5.2) becomes a homomorphism of commutative rings. This means that the operations

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab] \quad (5.3)$$

provide X with a well-defined commutative ring structure. If so, then the zero element of X is the class of zero $[0]$. Therefore, $[0] = \ker \pi \subset K$ should be an ideal in K , and by [Proposition 2.1](#) on p. 32, every fiber $[a] = \pi^{-1}(\pi(a))$ of the homomorphism (5.2) is the parallel shift of $[0]$ by a :

$$\forall a \in K, \quad [a] = a + [0] = \{a + b \mid b \in [0]\}.$$

In fact, these necessary conditions are also sufficient: for every ideal $I \subset K$, the *congruence modulo I* relation $a_1 \equiv a_2 \pmod{I}$, meaning that $a_1 - a_2 \in I$, is an equivalence on K . It decomposes K into a disjoint union of *residues*² modulo I ,

$$[a]_I \stackrel{\text{def}}{=} a + I = \{a + b \mid b \in I\}, \quad (5.4)$$

and the operations (5.3) provide the set of residues X with the well-defined structure of a commutative ring with zero element $[0]_I = I$ and unit element $[1]_I$ (if there is a unit $1 \in K$).

Exercise 5.8 Check that congruence modulo I is an equivalence relation and verify that the operations (5.3) are well defined on the equivalence classes (5.4).

¹That is, all power series converging everywhere in \mathbb{C} .

²Also called *cosets* of the ideal I .

Definition 5.2 For a commutative ring K and ideal $I \subset K$, the ring of residues (5.4) equipped with the operations (5.3) is called the *quotient ring* (or *factor ring*) of K modulo I and is denoted by K/I . The surjective homomorphism of rings

$$K \twoheadrightarrow K/I, \quad a \mapsto [a]_I, \quad (5.5)$$

is called the *quotient homomorphism*.

For example, the residue rings $\mathbb{Z}/(n)$ and $\mathbb{k}[x]/(f)$ are the quotient rings of \mathbb{Z} and $\mathbb{k}[x]$ modulo the principal ideals $(n) \subset \mathbb{Z}$ and $(f) \subset \mathbb{k}[x]$.

Example 5.2 (Image of a Ring Homomorphism) It follows from Sect. 2.6.4 on p. 33 that the image of a ring homomorphism $\varphi : K_1 \rightarrow K_2$ is isomorphic to the quotient ring $K_1 / \ker(\varphi)$. The isomorphism sends an element $b = \varphi(a) \in \text{im } \varphi$ to the coset $[a]_{\ker \varphi} = \varphi^{-1}(b)$. Therefore, every homomorphism of rings $\varphi : K_1 \rightarrow K_2$ can be decomposed as the quotient epimorphism $K_1 \twoheadrightarrow K_1 / \ker \varphi$ followed by the monomorphism $K_1 / \ker \varphi \simeq \text{im } \varphi \hookrightarrow K_2$.

Exercise 5.9 Show that every quotient ring of a Noetherian ring is Noetherian.

5.2.2 Maximal Ideals and Evaluation Maps

An ideal $\mathfrak{m} \subset K$ is said to be *maximal* if the quotient ring K/\mathfrak{m} is a field. This is equivalent to saying that \mathfrak{m} is maximal among the proper ideals³ partially ordered by inclusion. Indeed, the nontriviality axiom $0 \neq 1$ holds in K/\mathfrak{m} if and only if $1 \notin \mathfrak{m}$. The class $[a] \neq [0]$ is invertible in K/\mathfrak{m} if and only if there exist $b \in K$, $x \in \mathfrak{m}$ such that $ab = 1 + x$ in K , meaning that the ideal spanned by \mathfrak{m} and $a \in K \setminus \mathfrak{m}$ contains 1 and coincides with K . Thus, the invertibility of a nonzero class in K/\mathfrak{m} means that \mathfrak{m} cannot be enlarged within the class of proper ideals by adding an element from $K \setminus \mathfrak{m}$.

For a proper ideal $J \subset K$, write $\mathcal{I}(J)$ for the set of all proper ideals $J \supset I$. It is partially ordered by inclusion and complete,⁴ because every chain of ideals $I_\nu \in \mathcal{I}$ has an upper bound $I = \bigcup I_\nu$.

Exercise 5.10 Check that I is a proper ideal of K .

By Zorn's lemma, Lemma 1.3, $\mathcal{I}(J)$ contains a maximal element, and the above arguments show that every such element is a maximal ideal in K . Therefore, every proper ideal is contained in some maximal ideal. Note that every field contains just one maximal ideal, the zero ideal (0) .

³That is, among ideals different from K itself.

⁴See Definition 1.2 on p. 16.

Maximal ideals appear in rings of functions as the kernels of *evaluation maps*. Given a set X and a field \mathbb{k} , write $K = \mathbb{k}^X$ for the ring of all functions $f : X \rightarrow \mathbb{k}$. Then associated with an arbitrary point $p \in X$ is the evaluation map sending the function $f : X \rightarrow \mathbb{k}$ to its value at p :

$$\text{ev}_p : K \rightarrow \mathbb{k}, \quad f \mapsto f(p).$$

It is obviously surjective. Hence, in accordance with Example 5.2, $K/\ker \text{ev}_p \simeq \text{im } \text{ev}_p = \mathbb{k}$ is a field. Therefore, $\ker \text{ev}_p = \{f \in K \mid f(p) = 0\}$ is a maximal ideal in K .

Exercise 5.11 Show that every maximal ideal in $\mathbb{C}[x]$ coincides with $\ker \text{ev}_p$ for some $p \in \mathbb{C}$ and determine a maximal ideal $\mathfrak{m} \subset \mathbb{R}[x]$ different from all the ideals $\ker \text{ev}_p$ for $p \in \mathbb{R}$.

Exercise 5.12 Show that the maximal ideals in the ring of continuous functions $[0, 1] \rightarrow \mathbb{R}$ are exhausted by $\ker \text{ev}_p$ for $p \in [0, 1]$.

5.2.3 Prime Ideals and Ring Homomorphisms to Fields

An ideal $\mathfrak{p} \subset K$ is said to be *prime* if the quotient ring K/\mathfrak{p} has no zero divisors. In other words, $\mathfrak{p} \subset K$ is prime if for all $a, b \in K$, the inclusion $ab \in \mathfrak{p}$ implies that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. For example, the principal ideals $(p) \subset \mathbb{Z}$ and $(q) \subset \mathbb{k}[x]$ are prime if and only if $p \in \mathbb{Z}$ is a prime number and $q \in \mathbb{k}[x]$ is an irreducible polynomial.

Exercise 5.13 Prove the last two assertions.

It follows from the definitions that every maximal ideal is prime. The converse is not true in general. For example, the principal ideal $(x) \subset \mathbb{Q}[x, y]$ is prime but not maximal, because $\mathbb{Q}[x, y]/(x) \simeq \mathbb{Q}[y]$ is an integral domain but not a field. The prime ideals of a ring K are the kernels of nonzero homomorphisms

$$\varphi : K \rightarrow \mathbb{k},$$

where \mathbb{k} is an arbitrary field. Indeed, the image $\text{im } \varphi \simeq K/\ker \varphi$ of any such homomorphism is an integral domain, because the ambient field \mathbb{k} is. Conversely, if K/\mathfrak{p} is an integral domain, then it admits a canonical embedding

$$\iota : K/\mathfrak{p} \hookrightarrow Q_{K/\mathfrak{p}}$$

into its field of fractions. The quotient map $\pi : K \twoheadrightarrow K/\mathfrak{p}$ followed by this embedding is a homomorphism of rings $\iota\pi : K \rightarrow Q_{K/\mathfrak{p}}$ with kernel \mathfrak{p} .

Exercise 5.14 Assume that a prime ideal \mathfrak{p} contains the intersection of ideals I_1, I_2, \dots, I_m . Prove that at least one of the ideals I_k is completely contained in \mathfrak{p} .

5.2.4 Finitely Generated Commutative Algebras

Given a commutative ring K with unit, a quotient ring of the form

$$A = K[x_1, x_2, \dots, x_n]/I,$$

where $I \subset K[x_1, x_2, \dots, x_n]$ is an arbitrary ideal, is called a *finitely generated K -algebra*.⁵ The residue classes $a_i = x_i \pmod{I}$ are called *generators* of A . Polynomials $f \in I$ are called *relations* between the generators. Informally, a K -algebra A consists of all polynomial expressions produced by means of commuting letters a_1, a_2, \dots, a_n and the elements of K using addition, subtraction, and multiplication in the presence of polynomial relations $f(a_1, a_2, \dots, a_n) = 0$ for all $f \in I$.

Corollary 5.3 *Every finitely generated commutative algebra A over a Noetherian ring K is Noetherian, and all polynomial relations between generators of A follow from some finite set of those relations.*

Proof The result follows immediately from [Exercise 5.9](#) and [Corollary 5.1](#). \square

5.3 Principal Ideal Domains

5.3.1 Euclidean Domains

Definition 5.3 (Principal Ideal Domain) An integral domain⁶ K is called a *principal ideal domain* if every ideal in K is a principal ideal, that is, if it is generated by a single element.

For example, \mathbb{Z} and $\mathbb{k}[x]$ are principal ideal domains. We essentially proved this when we constructed the GCD in these rings.⁷ The key point in the proofs was a *division with remainder* argument, which can be formalized as follows.

Definition 5.4 (Euclidean Domain) An integral domain K is called *Euclidean* if K is equipped with a *degree function*⁸ $v : K \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ such that for all $a, b \in K \setminus 0$,

⁵Or more solemnly, a *finitely generated commutative algebra over K* .

⁶That is, a commutative ring with unit and without zero divisors (see [Sect. 2.4.2](#) on p. 28).

⁷See [Sect. 2.2.2](#) on p. 24 and [Proposition 3.4](#) on p. 47.

⁸Also called a *Euclidean valuation*.

the inequality $v(ab) \geq v(a)$ holds and

$$\exists q, r \in K : a = bq + r \text{ and either } v(r) < v(b) \text{ or } r = 0. \quad (5.6)$$

The elements q, r in (5.6) are called the *quotient* and *remainder* of the division of a by b . Note that the definition does not require the uniqueness of q, r for given a, b .

Exercise 5.15 Verify that the following rings with degree functions are Euclidean:

- (a) \mathbb{Z} , $v(z) = |z|$, (b) $\mathbb{k}[x]$, $v(f) = \deg f$,
- (c) $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}, i^2 = -1\}$, $v(z) = |z|^2$,
- (d) $\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z}, \omega^2 + \omega + 1 = 0\}$, $v(z) = |z|^2$.

Theorem 5.2 Every Euclidean domain K is a principal ideal domain.

Proof Given a nonzero ideal $I \subset K$, write $d \in I$ for some nonzero element of lowest degree. Clearly, $(d) \subset I$. Each $a \in I$ can be written as $a = dq + r$, where either $r = 0$ or $v(r) < v(d)$. The latter is impossible by the choice of d , because $r = a - dq \in I$. Hence, $r = 0$, and therefore $I \subset (d)$. \square

Corollary 5.4 The rings \mathbb{Z} , $\mathbb{k}[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ from Exercise 5.15 are principal ideal domains.

Caution 5.2 There are non-Euclidean principal ideal domains. Among the simplest examples are the ring $\mathbb{R}[x, y]/(x^2 + y^2 + 1)$ and the ring of algebraic numbers of the form $(x + y\sqrt{-19})/2$, where $x, y \in \mathbb{Z}$ are either both even or both odd. However, a thoroughgoing discussion of such examples requires advanced techniques from number theory and geometry that would take us outside the scope of this book.

Exercise 5.16 Let K be a Euclidean domain. Prove that a nonzero element $b \in K$ is invertible if and only if $v(ab) = v(a)$ for all nonzero $a \in K$.

5.3.2 Greatest Common Divisor

Let K be an arbitrary principal ideal domain. For a finite set of elements $a_1, a_2, \dots, a_n \in K$, there exists an element $d \in K$ such that d divides each a_i and is divisible by every common divisor of all the a_i . It is called a *greatest common divisor* and denoted by $\text{GCD}(a_1, a_2, \dots, a_n)$. By definition, d is a greatest common divisor of $a_1, a_2, \dots, a_n \in K$ if and only if $(d) = (a_1, a_2, \dots, a_n) = \{x_1 a_1 + x_2 a_2 + \dots + x_n a_n \mid x_i \in K\}$. The following exercise shows that any two greatest common divisors differ by an invertible factor.

Exercise 5.17 (Associated Elements) Prove that the following properties of nonzero elements a, b of an integral domain K are equivalent: **(a)** $(a) = (b)$, **(b)** $a \mid b$ and $b \mid a$, **(c)** $a = sb$ for some invertible $s \in K$.

Elements a, b satisfying the conditions of [Exercise 5.17](#) are called *associates*. For example, integers $a, b \in \mathbb{Z}$ are associates if and only if $a = \pm b$. Thus, the notation $\text{GCD}(a_1, a_2, \dots, a_n)$ means a class of mutually associated elements. Note that every greatest common divisor d , as an element of the ideal (a_1, a_2, \dots, a_n) , admits a representation $d = x_1a_1 + x_2a_2 + \dots + x_na_n$, where $x_i \in K$.

5.3.3 Coprime Elements

It follows from the previous section that the following conditions on a collection of elements a_1, a_2, \dots, a_n in a principal ideal domain K are equivalent:

- Every common divisor of a_1, a_2, \dots, a_n is invertible.
- $x_1a_1 + x_2a_2 + \dots + x_na_n = 1$ for some $x_i \in K$.
- $(a_1, a_2, \dots, a_n) = K$.

Elements a_1, a_2, \dots, a_n satisfying these conditions are called *coprime*.⁹

5.3.4 Irreducible Elements

Recall¹⁰ that a noninvertible element $q \in K$ is *irreducible* if the factorization $q = ab$ is possible only if a or b is invertible. Equivalently, $q \in K$ is irreducible if and only if the ideal (q) is maximal among the proper principal ideals partially ordered by inclusion. In a principal ideal domain, two irreducible elements p, q are either associates or coprime. Indeed, $(p, q) = (d)$ for some d , and there are two possibilities: either d is invertible or d is associated with both p and q . In the first case, $(p, q) \ni 1$, and therefore p, q are coprime.

Caution 5.3 In an integral domain K that is not a principal ideal domain, two unassociated irreducible elements are not necessarily coprime. For example, the polynomials $x, y \in \mathbb{Q}[x, y]$ are irreducible, unassociated, and not coprime.

Exercise 5.18 Check that the ideals $(x, y) \subset \mathbb{Q}[x, y]$ and $(2, x) \in \mathbb{Z}[x]$ are not principal.

⁹See Sect. 2.7 on p. 34.

¹⁰See Definition 3.3 on p. 48.

Proposition 5.2 *The following properties of an element p in a principal ideal domain K are equivalent:*

- (1) *The quotient ring $K/(p)$ is a field.*
- (2) *The quotient ring $K/(p)$ has no zero divisors.*
- (3) *The element p is irreducible.*

Proof The implication (1) \Rightarrow (2) holds trivially for every commutative ring¹¹ K . The implication (2) \Rightarrow (3) holds for every integral domain¹² K . Indeed, if $p = ab$ in K , then $[a][b] = 0$ in $K/(p)$. Since $K/(p)$ has no zero divisors, one of the two factors, say $[a]$, equals $[0]$. Therefore, $a = ps = abs$ for some $s \in K$. This leads to $a(1 - bs) = 0$ and $bs = 1$. Hence, b is invertible. It remains to establish the implication (3) \Rightarrow (1) for every principal ideal domain K . As soon as all ideals in K are principal, maximality of (p) among proper principal ideals means maximality among all proper ideals, which in turn means that $K/(p)$ is a field, as we have seen in Sect. 5.2.2 on p. 107. \square

5.4 Unique Factorization Domains

Throughout this section, we denote by K an arbitrary integral domain, that is, a commutative ring with unit and without zero divisors.

5.4.1 Irreducible Factorization

Proposition 5.3 *If K is Noetherian, then every noninvertible element $a \in K$ is a finite product of irreducible elements.*

Proof If a is irreducible, there is nothing to do. If not, we write a as a product of two noninvertible elements and repeat the process on each factor. If this procedure stops after a finite number of iterations, we get the required irreducible factorization. If not, we can form an infinite sequence of elements $a = a_0, a_1, a_2, \dots$ in which a_{i+1} divides a_i but is not an associate of a_i . This means that the principal ideals $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$ form an infinite strictly increasing tower, which cannot exist in a Noetherian ring. \square

Definition 5.5 (Unique Factorization Domain) An integral domain K is called a *unique factorization domain* if every noninvertible element of K is a finite product of irreducible elements and every equality $p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_n$ between such products implies that $m = n$ and the factors can be renumbered in such a way

¹¹See Sect. 2.4.2 on p. 28.

¹²Not necessarily a principal ideal domain.

that $q_v = p_v s_v$ for some invertible $s_v \in K$ for all v . A factorization $a = q_1 \cdot q_2 \cdots q_m$ in which all q_v are irreducible is called an *irreducible factorization* of a . Its factors q_i are called *irreducible factors* of a . Note that such factors are defined only up to multiplication by an invertible element of K .

Example 5.3 (Integers) The ring \mathbb{Z} is a unique factorization domain by [Exercise 2.8](#). In \mathbb{Z} , each class of associated irreducible elements contains a canonical representative, the *positive* prime p . Choosing these canonical irreducible elements, we can provide each integer n with the canonical irreducible factorization $n = \pm p_1 \cdot p_2 \cdots p_m$, where p_1, p_2, \dots, p_m are nondecreasing positive prime numbers. Such a canonical factorization is *uniquely* determined by n , with no ambiguity whatsoever.

Example 5.4 (Polynomials with Coefficients in a Field) For a field \mathbb{k} , the polynomial ring $\mathbb{k}[x]$ is a unique factorization domain by [Exercise 3.7](#). In $\mathbb{k}[x]$, each class of associated irreducible elements also contains a canonical representative, the *monic* irreducible polynomial. In choosing these canonical irreducibles, we can provide a polynomial f with an irreducible factorization $f = c p_1 \cdot p_2 \cdots p_m$, where $c \in \mathbb{k}$ and p_1, p_2, \dots, p_m are monic irreducible polynomials. Such a factorization is determined by f up to a permutation of the p_i .

Example 5.5 (Non-unique Factorization Domain) The ring $\mathbb{Z}[\sqrt{5}] \stackrel{\text{def}}{=} \mathbb{Z}[x]/(x^2 - 5)$ consists of elements $a + b\sqrt{5}$, where $a, b \in \mathbb{Z}$ and $\sqrt{5} \stackrel{\text{def}}{=} [x]$ satisfies $\sqrt{5} \cdot \sqrt{5} = 5$. It is isomorphic to the smallest subring of \mathbb{R} containing \mathbb{Z} and the number $\sqrt{5} \in \mathbb{R}$. Let us verify that the following two factorizations of the number 4 within $\mathbb{Z}[\sqrt{5}]$,

$$2 \cdot 2 = 4 = (\sqrt{5} + 1) \cdot (\sqrt{5} - 1) \quad (5.7)$$

are distinct irreducible factorizations. In analogy with the complex numbers, let us call the elements $\vartheta = a + b\sqrt{5}$ and $\bar{\vartheta} = a - b\sqrt{5}$ *conjugates* and introduce the *norm* $\|\vartheta\| \stackrel{\text{def}}{=} \vartheta \cdot \bar{\vartheta} = a^2 - 5b^2 \in \mathbb{Z}$.

Exercise 5.19 Verify that conjugation $\vartheta \mapsto \bar{\vartheta}$ is a ring automorphism of $\mathbb{Z}[\sqrt{5}]$.

The above exercise implies that the norm is multiplicative: $\|\vartheta_1 \vartheta_2\| = \vartheta_1 \vartheta_2 \bar{\vartheta}_1 \bar{\vartheta}_2 = \|\vartheta_1\| \cdot \|\vartheta_2\|$. In particular, $\vartheta \in \mathbb{Z}[\sqrt{5}]$ is invertible if and only if $\|\vartheta\| = \pm 1$, and in this case, $\vartheta^{-1} = \pm \bar{\vartheta}$. Since $\|2\| = 4$ and $\|\sqrt{5} \pm 1\| = -4$, factorization of these elements as a product xy of noninvertible x, y forces $\|x\| = \|y\| = \pm 2$. However, in $\mathbb{Z}[\sqrt{5}]$ there are no elements of norm ± 2 , because the equation $a^2 - 5b^2 = \pm 2$ has no integer solutions. Indeed, the residues of both sides modulo 5 satisfy $a^2 = \pm 2$ in \mathbb{F}_5 , but neither $+2$ nor -2 is a square in \mathbb{F}_5 . We conclude that 2 and $\sqrt{5} \pm 1$ are irreducible in $\mathbb{Z}[\sqrt{5}]$. Since neither $\sqrt{5} + 1$ and $\sqrt{5} - 1$ is divisible by 2 in $\mathbb{Z}[\sqrt{5}]$, the two irreducible factorizations (5.7) are actually different.

5.4.2 Prime Elements

An element $p \in K$ is called *prime* if the principal ideal $(p) \subset K$ is prime, that is, if the quotient ring $K/(p)$ has no zero divisors. In other words, p is prime if and only if the condition $p \mid ab$ implies that $p \mid a$ or $p \mid b$. Every prime element p is irreducible. Indeed, if $p = xy$, then one of the factors, say x , is divisible by p . Hence, $p = pyz$ for some z . This forces $yz = 1$ and means that y is invertible.

We know from Proposition 5.2 on p. 111 that in a principal ideal domain, the converse is also true: every irreducible element is prime. However, in an integral domain that has nonprincipal ideals, an irreducible element may be not prime. For example, in $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2 - 5)$, the element 2 is irreducible but not prime, because the quotient ring

$$\begin{aligned} \mathbb{Z}[\sqrt{5}]/(2) &\simeq \mathbb{Z}[x]/(2, x^2 - 5) = \mathbb{Z}[x]/(2, x^2 + 1) \simeq \mathbb{F}_2[x]/(x^2 + 1) \\ &\simeq \mathbb{F}_2[x]/((x + 1)^2) \end{aligned}$$

has the zero divisor $(x + 1) \pmod{(2, x^2 + 1)}$. In particular, this means that the *irreducible* number 2 does not divide $1 + \sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$ but divides $(1 + \sqrt{5})^2 = 6 + 2\sqrt{5}$.

Proposition 5.4 *A Noetherian integral domain K is a unique factorization domain if and only if every irreducible element in K is prime.*

Proof Let K be a unique factorization domain and $q \in K$ irreducible. If q divides some product ab , then an irreducible factorization of ab contains a factor associated with q . On the other hand, an irreducible factorization of ab is the product of irreducible factorizations of a and b . Thanks to unique factorization, q is associated with some irreducible factor in a or in b . Therefore, q divides a or b .

Now suppose all irreducible elements of K are prime. We know from Proposition 5.3 that every element of a Noetherian ring admits an irreducible factorization. Let us prove that in every integral domain, an equality between two products of prime elements

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m \tag{5.8}$$

implies that $k = m$ and (after appropriate renumbering) $q_i = s_i p_i$ for some invertible s_i for each i . Since p_1 divides the right-hand side of (5.8), one of the factors there, say q_1 , is divisible by p_1 . Therefore, $q_1 = s_1 p_1$, where s_1 is invertible, because q_1 is irreducible. Since K has no zero divisors, we can cancel the factor p_1 on the both sides of (5.8) and repeat the argument for the shorter equality $p_2 p_3 \cdots p_k = (s_1 q_2) q_3 \cdots q_m$. \square

Corollary 5.5 *Every principal ideal domain is a unique factorization domain.*

Proof This follows at once from Proposition 5.2 on p. 111 □

Example 5.6 (Sums of Two Squares, Continuation of Sect. 3.5.5) It follows from the previous corollary and Corollary 5.4 that the ring of Gaussian integers $\mathbb{Z}[i]$ is a unique factorization domain. Let us ascertain whether a given prime $p \in \mathbb{N}$ remains irreducible in $\mathbb{Z}[i]$. Since $\bar{p} = p$ and p has no real irreducible divisors that are not associates of p , all the factors in an irreducible factorization of p in $\mathbb{Z}[i]$ split into pairs of complex conjugate divisors. Therefore, a prime $p \in \mathbb{Z}$ that becomes reducible in $\mathbb{Z}[i]$ can be written as $p = (a + ib)(a - ib) = a^2 + b^2$ with nonzero $a, b \in \mathbb{Z}$. In other words, a prime $p \in \mathbb{N}$ is reducible in $\mathbb{Z}[i]$ if and only if p is a sum of two perfect squares. At the same time, a prime $p \in \mathbb{Z}[i]$ is irreducible in $\mathbb{Z}[i]$ if and only if the quotient ring $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2 + 1) \simeq \mathbb{F}_p[x]/(x^2 + 1)$ is a field.¹³ This means that the quadratic binomial $x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$, that is, has no roots in \mathbb{F}_p . We conclude that a prime $p \in \mathbb{Z}$ is a sum of two squares if and only if -1 is a quadratic nonresidue modulo p . We have seen in Sect. 3.6.3 on p. 65 that the latter is the case if and only if $(p - 1)/2$ is even, that is, for primes $p = 4k + 1$ and $p = 2$.

Exercise 5.20 Use Sect. 3.5.5 on p. 62 and Example 5.6 to prove that a number $n \in \mathbb{N}$ is a sum of two perfect squares if and only if every prime factor of the form $p = 4k + 3$ appears in the prime factorization of n an even number of times.

5.4.3 GCD in Unique Factorization Domains

A finite collection of elements a_1, a_2, \dots, a_m in a unique factorization domain K has a greatest common divisor,¹⁴ which can be described as follows. Choose $q \in K$ in each class of associated irreducible elements and write m_q for the maximal power of q that divides all the elements a_i . Then up to multiplication by invertible elements,

$$\text{GCD}(a_1, a_2, \dots, a_m) = \prod_q q^{m_q}. \quad (5.9)$$

Since each a_i is divisible by only a finite number of q 's, all but a finite number of exponents m_q vanish. Therefore, the product on the right-hand side of (5.9) is finite. By construction, it divides each a_i . Since K is a unique factorization domain, every common divisor of all the elements a_i must divide the right-hand side of (5.9).

¹³See Proposition 5.2 on p. 111.

¹⁴See Remark 2.3 on p. 27.

5.4.4 Polynomials over Unique Factorization Domains

Let K be a unique factorization domain with field of fractions¹⁵ \mathcal{Q}_K . The polynomial ring $K[x]$ is a subring of the polynomial ring $\mathcal{Q}_K[x]$. Given a polynomial

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in K[x], \quad (5.10)$$

we write $\text{cont}(f) \stackrel{\text{def}}{=} \text{GCD}(a_0, a_1, \dots, a_n) \in K$ for the greatest common divisor of the coefficients and call it the *content* of the polynomial f . The content of a polynomial is defined up to multiplication by invertible elements.

Lemma 5.2 *For all $f, g \in K[x]$, the equality $\text{cont}(fg) = \text{cont}(f) \cdot \text{cont}(g)$ holds.*

Proof Since K is a unique factorization domain, it is enough to check that for every irreducible $q \in K$, the following statement holds: q divides $\text{cont}(fg)$ if and only if q divides $\text{cont}(f) \cdot \text{cont}(g)$. Since every irreducible element is prime in a unique factorization domain, the quotient ring $R = K/(q)$ has no zero divisors. For the polynomial (5.10), write $[f]_q(x) = [a_0]_qx^n + [a_1]_qx^{n-1} + \cdots + [a_{n-1}]_qx + [a_n]_q \in R[x]$ for the polynomial whose coefficients are the residues of the coefficients of f modulo q . Then the map $K[x] \rightarrow R[x], f \mapsto [f]_q$, is a ring homomorphism. Since $R[x]$ is an integral domain, the product $[fg]_q = [f]_q[g]_q$ equals zero if and only if one of the factors $[f]_q, [g]_q$ equals zero. In other words, q divides all coefficients of fg if and only if q divides all coefficients of g or all coefficients of f . \square

Lemma 5.3 (Simplified Form of a Polynomial) *Every polynomial $f(x) \in \mathcal{Q}_K[x]$ can be written as*

$$f(x) = \frac{a}{b} \cdot f_{\text{red}}(x), \quad (5.11)$$

where $f_{\text{red}} \in K[x]$, $a, b \in K$, and $\text{cont}(f_{\text{red}}) = \text{GCD}(a, b) = 1$. The elements a, b and the polynomial f_{red} are determined by f uniquely up to multiplication by invertible elements of K .

Proof Factor the lowest common denominator from the coefficients of f . Then factor out the greatest common divisor from the numerators. We get a number $c \in \mathcal{Q}_K$ multiplied by a polynomial of content 1 with coefficients in K . Denote this polynomial by $f_{\text{red}} \in K[x]$ and write c as a simplified fraction a/b . This is the representation (5.11). Given an equality of the expressions for (5.11) in $\mathcal{Q}_K[x]$,

$$\frac{a}{b} \cdot f_{\text{red}}(x) = \frac{c}{d} \cdot g_{\text{red}}(x),$$

then $ad \cdot f_{\text{red}}(x) = bc \cdot g_{\text{red}}(x)$ in $K[x]$. A comparison of the contents of both sides leads to the equality $ad = bc$. Since $\text{GCD}(a, b) = \text{GCD}(c, d) = 1$, the elements

¹⁵See Sect. 4.1.2 on p. 75.

a, c should be associates, as should also b, d . This forces $f_{\text{red}}(x) = g_{\text{red}}(x)$ up to multiplication by an invertible constant from K . \square

Lemma 5.4 (Gauss's Lemma) *Every irreducible polynomial $f \in K[x]$ remains irreducible in $Q_K[x]$.*

Proof Since f is irreducible, $\text{cont}(f) = 1$. Let $f(x) = g(x) \cdot h(x)$ in $Q_K[x]$. Write g and h in the simplified form (5.11) and simplify the resulting constant factor. Then we get the equality

$$f(x) = \frac{a}{b} \cdot g_{\text{red}}(x) \cdot h_{\text{red}}(x), \quad (5.12)$$

where $g_{\text{red}}, h_{\text{red}} \in K[x]$ have content 1, and $a, b \in K$ have $\text{GCD}(a, b) = 1$. By Lemma 5.2,

$$\text{cont}(g_{\text{red}}h_{\text{red}}) = \text{cont}(g_{\text{red}}) \cdot \text{cont}(h_{\text{red}}) = 1.$$

Therefore, the right-hand side of (5.12) is the simplified expression (5.11) for f . By Lemma 5.3, both elements a, b are invertible in K , and $f = g_{\text{red}}h_{\text{red}}$ up to multiplication by invertible elements of K . \square

Theorem 5.3 *If K is a unique factorization domain, then the polynomial ring $K[x]$ is a unique factorization domain as well.*

Proof Since the principal ideal domain $Q_K[x]$ is a unique factorization domain, every $f \in K[x]$ is factorized within $Q_K[x]$ into a finite product of irreducible polynomials $f_v \in Q_K[x]$. If we write each f_v in simplified form (5.11) and reduce the resulting constant factor, we obtain the equality

$$\text{cont}(f) \cdot f_{\text{red}} = \frac{a}{b} \prod_v f_{v,\text{red}}, \quad (5.13)$$

where all the $f_{v,\text{red}} \in K[x]$ are irreducible of content 1, and $a, b \in K$ have $\text{GCD}(a, b) = 1$. Both sides of (5.13) have simplified form (5.11), because we have $\text{cont}(\prod_v f_{v,\text{red}}) = 1$. Therefore, $b = 1$ and $f = a \prod_v f_{v,\text{red}}$ up to multiplication by invertible elements of K . To get an irreducible factorization of f in $K[x]$, it remains to factorize $a \in K$ within K . Let us verify that the irreducible factorization in $K[x]$ is unique. Consider the equality $a_1 a_2 \cdots a_k \cdot p_1 p_2 \cdots p_s = b_1 b_2 \cdots b_m \cdot q_1 q_2 \cdots q_r$, where $a_\alpha, b_\beta \in K$ are irreducible constants and $p_\mu, q_\nu \in K[x]$ are irreducible polynomials. Since irreducible polynomials have content 1, a comparison of the contents of both sides leads to the equality $a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_m$ in K . Since K is a unique factorization domain, $k = m$, and (after appropriate renumbering) $a_i = s_i b_i$ for some invertible $s_i \in K$. Hence, $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$ in $K[x]$ up to multiplication by invertible elements of K . Since p_i, q_i are irreducible in $Q_K[x]$ and $Q_K[x]$ is a unique factorization domain, we conclude that $r = s$ and (after appropriate renumbering)

$p_i = q_i$ up to a constant factor. By Lemma 5.3, these factors have to be invertible elements of K . \square

Corollary 5.6 *If K is a unique factorization domain,¹⁶ then the polynomial ring $K[x_1, x_2, \dots, x_n]$ is also a unique factorization domain.* \square

5.5 Factorization of Polynomials with Rational Coefficients

In this section, we discuss how an irreducible factorization of a given polynomial $f \in \mathbb{Q}[x]$ can be obtained in practice. It is quite reasonable to begin with a determination of the rational roots of f . This can be done using a finite number of tests.

Exercise 5.21 Show that the simplified fraction $a = p/q \in \mathbb{Q}$ can be a root of the polynomial $a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in \mathbb{Z}[x]$ only if $p \mid a_0$ and $q \mid a_n$.

An explicit knowledge of the complex roots is also extremely helpful.

Exercise 5.22 Factorize $x^4 + 4$ as a product of two quadratic trinomials in $\mathbb{Z}[x]$.

After these simple considerations have been exhausted, one can invoke some deeper divisibility criteria. To apply them, we write f as $c \cdot g$, where $c \in \mathbb{Q}$ and $g \in \mathbb{Z}[x]$ has content 1. Then by Gauss's lemma,¹⁷ the factorization of f in $\mathbb{Q}[x]$ is equivalent to the factorization of g in $\mathbb{Z}[x]$. Let us analyze the factorization in $\mathbb{Z}[x]$.

5.5.1 Reduction of Coefficients

For $m \in \mathbb{Z}$, there is a homomorphism of rings

$$\mathbb{Z}[x] \rightarrow (\mathbb{Z}/(m))[x], \quad f \mapsto [f]_m, \quad (5.14)$$

which sends $a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x]$ to the polynomial

$$[a_n]_m x^n + [a_{n-1}]_m x^{n-1} + \dots + [a_1]_m x + [a_0]_m$$

with coefficients in the residue class ring $\mathbb{Z}/(m)$. The homomorphism (5.14) is called a *reduction of the coefficients*¹⁸ modulo m . Since the equality $f = gh$ in $\mathbb{Z}[x]$ implies the equality $[f]_m = [g]_m \cdot [h]_m$ in the ring $(\mathbb{Z}/(m))[x]$ for all m , the irreducibility of $[f]_m$ for some m forces f to be irreducible in $\mathbb{Z}[x]$. For prime $m = p$,

¹⁶In particular, a principal ideal domain or field.

¹⁷See Lemma 5.4 on p. 117.

¹⁸We have used this already in the proof of Lemma 5.2 on p. 116.

the residue class ring $\mathbb{Z}/(m)$ becomes the field \mathbb{F}_p , and the polynomial ring $\mathbb{F}_p[x]$ becomes a unique factorization domain. For small p and small degree of f , the irreducible factorization of f in $\mathbb{F}_p[x]$ can be carried out by simply running through all the irreducible polynomials in $\mathbb{F}_p[x]$. An analysis of such a factorization allows us to say something about the factorization of f in $\mathbb{Z}[x]$.

Example 5.7 Let us show that the polynomial $f(x) = x^5 + x^2 + 1$ is irreducible in $\mathbb{Z}[x]$. Since f has no integer roots, a nontrivial factorization $f = gh$ in $\mathbb{Z}[x]$ is possible only for $\deg(g) = 2$ and $\deg(h) = 3$. Reduction of the coefficients modulo 2 leads to the polynomial $[f]_2 = x^5 + x^2 + 1$, with no roots in \mathbb{F}_2 . This forces both $[g]_2$ and $[h]_2$ to be irreducible in $\mathbb{F}_2[x]$. Since $x^2 + x + 1$ is the only quadratic irreducible polynomial in $\mathbb{F}_2[x]$ and it does not divide $x^5 + x^2 + 1$ in $\mathbb{F}_2[x]$, we conclude that $[f]_2$ is irreducible in $\mathbb{F}_2[x]$. Hence, f is irreducible in $\mathbb{Z}[x]$ as well.

Example 5.8 (Eisenstein's Criterion) Assume that $f \in \mathbb{Z}[x]$ is monic and every coefficient of f except the leading coefficient is divisible by a prime $p \in \mathbb{N}$. Let $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$. Since reduction modulo p leads to $[f]_p(x) = x^n$, we conclude that $[g]_p(x) = x^k$, $[h]_p(x) = x^m$ for some k, m . This means that all but the leading coefficients of g, h are divisible by p as well. Hence, if both g and h are of positive degree, then the constant term of f must be divisible by p^2 . We conclude that a monic polynomial $f \in \mathbb{Z}[x]$ is irreducible if every coefficient of f except the leading coefficient is divisible by p and the constant term is not divisible by p^2 . This observation is known as *Eisenstein's criterion*.

Example 5.9 (Cyclotomic Polynomial Φ_p) Eisenstein's criterion allows us to see easily that for every prime $p \in \mathbb{N}$, the cyclotomic polynomial¹⁹

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

is irreducible in $\mathbb{Z}[x]$. Just pass to the new variable $t = x - 1$. Then

$$f(t) = \Phi_p(t+1) = \frac{(t+1)^p - 1}{t} = t^{p-1} + \binom{p}{1}t^{p-2} + \cdots + \binom{p}{p-1}$$

satisfies Eisenstein's criterion, because for $1 \leq k \leq p-1$, the binomial coefficients $\binom{p}{k}$ are divisible by p , and the last of them, equal to p , is not divisible by p^2 .

5.5.2 Kronecker's Algorithm

Kronecker's algorithm allows us to check whether $f \in \mathbb{Z}[x]$ is irreducible, and if it is not, to produce an irreducible factorization of f in $\mathbb{Z}[x]$ after a finite but quite laborious computation. Let $\deg f = 2n$ or $\deg f = 2n + 1$ for some $n \in \mathbb{N}$. If there

¹⁹See Sect. 3.5.4 on p. 60.

exists a nontrivial factorization $f = gh$ in $\mathbb{Z}[x]$, we can assume that $\deg h \leq n$. Choose $n + 1$ different integers $z_0, z_1, \dots, z_n \in \mathbb{Z}$, then list all collections of integers $d = (d_0, d_1, \dots, d_n)$ such that d_i divides $f(z_i)$, and for each collection, form the unique polynomial²⁰ $h_d \in \mathbb{Q}[x]$ such that $h_d(z_i) = d_i$ for all i :

$$h_d(x) = \sum_{i=0}^n d_i \cdot \prod_{v \neq i} \frac{(x - z_v)}{(z_i - z_v)}. \quad (5.15)$$

Clearly, the polynomial h , if it exists, is equal to one of the h_d that has integer coefficients. Therefore, to check whether f has a divisor of degree $\leq n$, it is enough to examine whether f is divisible by some $h_d \in \mathbb{Z}[x]$ from the finite list just constructed.

Problems for Independent Solution to Chap. 5

Problem 5.1 Find all positive integers n divisible by 30 and having exactly 30 positive integer divisors including 1 and n itself.

Problem 5.2 Find all rational roots of the polynomial $2x^4 - 7x^3 + 4x^2 - 2x - 3$.

Problem 5.3 Show that for every field \mathbb{k} , the ring $\mathbb{k}[[x]]$ is Euclidean with the degree function v taking a power series f to the degree of the lowest term in f .

Problem 5.4 Assume that ± 1 are the only common divisors of polynomials $f, g \in \mathbb{Z}[x]$. Can the quotient ring $\mathbb{Z}[x]/(f, g)$ be infinite?

Problem 5.5 (Sums and Products of Ideals) Show that for ideals I, J in a commutative ring, the intersection $I \cap J$, *product* $IJ \stackrel{\text{def}}{=} \{x_1y_1 + x_2y_2 + \dots + x_ny_n \mid x_i \in I, y_i \in J, n \in \mathbb{N}\}$, and *sum* $I + J \stackrel{\text{def}}{=} \{x + y \mid x \in I, y \in J\}$ are ideals as well. Prove that $IJ \subset I \cap J$ and give an example of $IJ \neq I \cap J$.

Problem 5.6 (Radical of an Ideal) Let K be an arbitrary commutative ring with unit. Given an ideal $I \subset K$, show that its *radical* $\sqrt{I} \stackrel{\text{def}}{=} \{a \in K \mid \exists n \in \mathbb{N} : a^n \in I\}$ is also an ideal and check that $\sqrt{IJ} = \sqrt{I \cap J}$ for all ideals $I, J \subset K$.

Problem 5.7 (Coprime Ideals) Ideals I, J of an arbitrary commutative ring K with unit are called *coprime* if $I + J = K$, i.e., there exist $x \in I, y \in J$ such that $x + y = 1$. Show that: **(a)** $IJ = I \cap J$ for all coprime I, J , **(b)** if I is coprime to every ideal in the collection J_1, J_2, \dots, J_n , then I and $\bigcap_v J_v$ are coprime.

Problem 5.8 (Chinese Remainder Theorem) Prove that for every commutative ring K with unit and every collection of mutually coprime ideals $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_m \subset K$, we have $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \dots \cdot \mathfrak{a}_m = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_m$, and construct an isomorphism

$$K/\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \dots \cdot \mathfrak{a}_m \simeq (K/\mathfrak{a}_1) \times (K/\mathfrak{a}_2) \times \dots \times (K/\mathfrak{a}_m).$$

²⁰See [Exercise 3.10](#) on p. 50.

Problem 5.9 Given a homomorphism of commutative rings $\varphi : K \rightarrow L$ and a polynomial $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in K[x]$, write f^φ for the polynomial $\varphi(a_n)x^n + \varphi(a_{n-1})x^{n-1} + \cdots + \varphi(a_0) \in L[x]$. Verify that the map

$$\hat{\varphi} : K[x] \rightarrow L[x], \quad f \mapsto f^\varphi,$$

is a ring homomorphism. Assume that both rings K, L are integral domains. Show that if f^φ is irreducible in $\mathbb{Q}_L[x]$ and $\deg f^\varphi = \deg f$, then f is irreducible in $K[x]$.

Problem 5.10 Determine whether the polynomial (a) $x^4 - 8x^3 + 12x^2 - 6x + 2$, (b) $x^5 - 12x^3 + 36x - 12$, is reducible in $\mathbb{Q}[x]$.

Problem 5.11 Determine whether the following polynomials are irreducible in $\mathbb{Z}[x]$ and find the irreducible factorizations of those that are reducible: (a) $x^4 + x + 1$, (b) $x^5 + x^4 + x^2 + x + 2$, (c) $x^6 + x^3 + 1$, (d) $x^{105} - 9$.

Problem 5.12 For an arbitrary collection of distinct integers $a_1, \dots, a_n \in \mathbb{Z}$, determine whether the given polynomial is irreducible in $\mathbb{Q}[x]$: (a) $(x - a_1)(x - a_2) \cdots (x - a_n) - 1$, (b) $(x - a_1)^2 \cdots (x - a_n)^2 + 1$.

Problem 5.13 Without using Zorn's lemma, show that every proper ideal of a Noetherian ring is contained in some maximal ideal.

Problem 5.14 List all ideals in the ring $\mathbb{k}[[t]]$, where \mathbb{k} is a field, and describe all the maximal ideals among them.

Problem 5.15 Find a nonprime irreducible element in the ring $\mathbb{Z}[\sqrt{13}]$.

Problem 5.16 Let \mathbb{k} be a field and $K \supset \mathbb{k}$ an integral domain. Given $\xi \in K$, write $\text{ev}_\xi : \mathbb{k}[x] \rightarrow K$ for the *evaluation map*, which sends $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{k}[x]$ to $f(\xi) = a_0\xi^n + a_1\xi^{n-1} + \cdots + a_{n-1}\xi + a_n \in K$. Show that (a) $\text{im}(\text{ev}_\xi)$ is the minimal subring in K containing \mathbb{k} and ξ , (b) $\text{im}(\text{ev}_\xi)$ is a field if and only if $\ker \text{ev}_\xi \neq 0$.

Problem 5.17 Among the quotient rings of $\mathbb{Z}[i]$, is there a field of characteristic (a) 2? (b) 3? If such a field exists, what can its cardinality be equal to?

Problem 5.18 Let $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ be prime ideals and I an arbitrary ideal such that $I \subset \bigcup_k \mathfrak{p}_k$. Prove that $I \subset \mathfrak{p}_k$ for some k .

Problem 5.19 Let K be a commutative ring with unit, $S \subset K$ a multiplicative set, $I \subset K$ an ideal such that $I \cap S = \emptyset$. Use Zorn's lemma to show that there exists an ideal $\mathfrak{p} \subset K$ maximal among ideals $J \subset K$ with $J \supseteq I$ and $J \cap S = \emptyset$, and every such \mathfrak{p} is prime.

Problem 5.20* (Nilradical). In a commutative ring K with unit, the radical of the zero ideal²¹ is called the *nilradical* of K and is denoted by

$$\mathfrak{n}(K) \stackrel{\text{def}}{=} \sqrt{(0)} = \{a \in K \mid a^n = 0 \text{ for some } n \in \mathbb{N}\}.$$

Show that $\mathfrak{n}(K)$ coincides with the intersection of all proper prime ideals $\mathfrak{p} \subset K$.

²¹Compare with Problem 5.6.

Problem 5.21* (Krull's Criterion). Show that an integral domain K is a unique factorization domain if and only if for every nonzero element $a \in K$, every minimal prime ideal²² $\mathfrak{p} \ni a$ is principal.

Problem 5.22 Let an integral domain K be equipped with a function

$$\mu : K \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$$

such that $\forall a, b \in K \setminus 0, \exists q, r \in K : a = bq + r$ and either $v(r) < v(b)$ or $r = 0$. Show that the function $v : K \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ defined by $v(a) \stackrel{\text{def}}{=} \min_{b \in K \setminus 0} (\mu(ab))$ is a Euclidean degree²³ on K .

²²That is, a prime ideal that does not contain prime ideals $\mathfrak{q} \subset \mathfrak{p}$ except for $\mathfrak{q} = \mathfrak{p}$ and $\mathfrak{q} = (0)$.

²³See Definition 5.4 on p. 109.

Chapter 6

Vectors

In this section we continue to use the notation of Chaps. 3–5 and write K for an arbitrary commutative ring with unit and \mathbb{k} for an arbitrary field.

6.1 Vector Spaces and Modules

6.1.1 Definitions and Examples

We begin with the definition of a vector space. It formalizes the algebraic properties of geometric vectors, namely the addition of vectors and the multiplication of vectors by constants. Although there is quite a variety of vector spaces—field extensions, function spaces, spaces of solutions of systems of linear equations, even spaces of subsets—it is useful to think of vectors as arrows considered up to a translation.

Definition 6.1 (Vector Space over \mathbb{k}) An additive abelian group V is called a *vector space* over a field \mathbb{k} if it is equipped with an operation

$$\mathbb{k} \times V \rightarrow V, \quad (\lambda, v) \mapsto \lambda v,$$

called *multiplication of vectors by scalars* and possessing the following properties:

$$\forall \lambda, \mu \in \mathbb{k}, \forall v \in V \quad \lambda(\mu v) = (\lambda\mu)v, \quad (6.1)$$

$$\forall \lambda, \mu \in \mathbb{k}, \forall v \in V \quad (\lambda + \mu)v = \lambda v + \mu v, \quad (6.2)$$

$$\forall v, w \in V, \forall \lambda \in \mathbb{k} \quad \lambda(v + w) = \lambda v + \lambda w, \quad (6.3)$$

$$\forall v \in V \quad 1 \cdot v = v. \quad (6.4)$$

The elements of the field \mathbb{k} are called *scalars*, and \mathbb{k} itself is referred to as the *ground field*. The elements of V are called *vectors*. The additive group operation $V \times V \rightarrow V$ is called *addition of vectors*. The neutral element $0 \in V$ is called the *zero vector*. A subset $U \subset V$ is called a *subspace* of V if it is itself a vector space with respect to the operations on V .

Definition 6.2 (K -Module) If the field \mathbb{k} in Definition 6.1 is replaced by an arbitrary commutative ring K and the property (6.4) is excluded, then an additive abelian group V equipped with multiplication by scalars $K \times V \rightarrow V$ satisfying the remaining conditions (6.1)–(6.3) is called a *module* over K or a *K -module* for short. If the ring K has a unit element and the property (6.4) is satisfied as well, then the K -module V is called *unital*.

Therefore, vector spaces are particular examples of unital modules.

Exercise 6.1 Deduce from (6.1)–(6.3) that $0 \cdot v = 0$ and $\lambda \cdot 0 = 0$ for all $v \in V$ and all $\lambda \in K$ in a K -module V . Show that for every unital module over a commutative ring with unit, $(-1) \cdot v = -v$ for all $v \in V$.

Agreement 6.1 Sometimes, it is more convenient to write $v\lambda$ instead of λv for the product of a vector $v \in V$ and scalar $\lambda \in K$. By definition, we put $v\lambda \stackrel{\text{def}}{=} \lambda v$ in a module V over a commutative ring K .

Example 6.1 (Zero Module) The simplest module is the *zero module* 0 , which consists of the zero vector only. The zero vector is opposite to itself, and $\lambda \cdot 0 = 0$ for all $\lambda \in K$.

Example 6.2 (Free Module of Rank 1 and Its Submodules) Every ring of scalars K is a K -module with respect to addition and multiplication in K . Such a module is called a *free module of rank 1*. The submodules of K are precisely the ideals $I \subset K$.

Example 6.3 (Abelian Groups) Every additive abelian group A has the natural structure of a \mathbb{Z} -module, in which multiplication by scalars is defined by

$$ma = \operatorname{sgn}(m) \cdot \underbrace{(a + a + \cdots + a)}_{|m| \text{ times}}.$$

The submodules of A coincide with the additive subgroups of A .

6.1.2 Linear Maps

Every map of K -modules $F : U \rightarrow W$ that respects addition and multiplication by scalars, that is, a map that satisfies for all $a, b \in U$ and all $\alpha, \beta \in K$ the condition

$$F(\alpha a + \beta b) = \alpha F(a) + \beta F(b),$$

is called a *homomorphism of K -modules* or, more frequently, a *linear map*.¹ We met linear maps $\mathbb{Q}[x] \rightarrow \mathbb{Q}[x]$ earlier in Sect. 4.4 on p. 88, when we studied the operators $\Phi(D)$ on the space of polynomials.

Two K -modules U, W are said to be *isomorphic* if there is a linear bijection $\varphi : U \xrightarrow{\sim} W$. Such a bijection is called an *isomorphism of K -modules*.

Since every linear map $F : U \rightarrow W$ is a homomorphism of abelian groups, it possesses all the properties of such homomorphisms.² In particular, $F(0) = 0$ and $F(-v) = -F(v)$ for all v . The image $\text{im } F = F(V) \subset W$ is a submodule of W , because $\lambda\varphi(u) = \varphi(\lambda u)$ for all $u \in U$. The kernel

$$\ker F = F^{-1}(0) = \{u \in U \mid F(u) = 0\}$$

is a submodule in U , because $\varphi(u) = 0$ forces $\varphi(\lambda u) = \lambda\varphi(u) = 0$. By Proposition 2.1 on p. 32, every nonempty fiber of F is a parallel shift of the kernel by any element of the fiber: $F^{-1}(F(u)) = u + \ker F = \{u + v \mid F(v) = 0\}$. Therefore, a linear map F is injective if and only if $\ker F = 0$.

Caution 6.1 Given $a, b \in K$, the map $\varphi : K \rightarrow K$, $\varphi(x) = a \cdot x + b$, which often is called a “linear function” in calculus, is linear in the sense of the above definition only for $b = 0$. If $b \neq 0$, then $\varphi(\lambda x) \neq \lambda\varphi(x)$ and $\varphi(x + y) \neq \varphi(x) + \varphi(y)$ for most x, y, λ . Thus in algebra, “linear” means what is called “linear homogeneous” in calculus.

6.1.3 Proportional Vectors

Let V be a vector space over a field \mathbb{k} . Vectors $a, b \in V$ are called *proportional*³ if $xa = yb$ for some $x, y \in \mathbb{k}$ such that $xy \neq 0$. Thus, the zero vector is proportional to every vector, whereas the proportionality of nonzero vectors a, b means that there exists a nonzero constant $\lambda \in \mathbb{k}$ such that $a = \lambda b$, or equivalently, $b = \lambda^{-1}a$.

Example 6.4 (Coordinate Plane) The simplest example of a nonzero vector space different from \mathbb{k} is the *coordinate plane* $\mathbb{k}^2 = \mathbb{k} \times \mathbb{k}$. By definition, it consists of ordered pairs of numbers arranged in columns of height two:

$$v = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \quad x_1, x_2 \in \mathbb{k}.$$

¹Or K -linear, if the precise reference on the ring of scalars is important.

²See Sect. 2.6 on p. 31.

³Also *collinear* or *linearly related*.

Addition and multiplication by scalars are defined componentwise:

$$\lambda \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + \mu \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} \lambda a_1 + \mu b_1 \\ \lambda a_2 + \mu b_2 \end{pmatrix}.$$

Vectors $a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ and $b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ are proportional if and only if $a_1 b_2 = a_2 b_1$. The difference

$$\det(a, b) \stackrel{\text{def}}{=} a_1 b_2 - a_2 b_1$$

is called the *determinant* of the vectors $a, b \in \mathbb{K}^2$. It is clear that

$$\det(a, b) = 0 \iff a \text{ and } b \text{ are proportional,} \quad (6.5)$$

$$\det(a, b) = -\det(b, a) \quad \forall a, b \in \mathbb{K}^2, \quad (6.6)$$

$$\det(\lambda a, b) = \lambda \det(a, b) = \det(a, \lambda b) \quad \forall a, b \in \mathbb{K}^2, \lambda \in \mathbb{K}, \quad (6.7)$$

$$\det(a_1 + a_2, b) = \det(a_1, b) + \det(a_2, b), \quad (6.8)$$

$$\det(a, b_1 + b_2) = \det(a, b_1) + \det(a, b_2) \quad \forall a, a_1, a_2, b, b_1, b_2 \in \mathbb{K}^2. \quad (6.9)$$

Properties (6.6), (6.7), and (6.9) are referred to as *skew symmetry*, *homogeneity*, and *additivity* respectively. Homogeneity and additivity together mean that the determinant is linear in each argument when the other is fixed, i.e., for all $a, b \in V$, the functions

$$\begin{aligned} \det(*, b) : V &\rightarrow \mathbb{K}, & v &\mapsto \det(v, b) \\ \det(a, *) : V &\rightarrow \mathbb{K}, & v &\mapsto \det(a, v) \end{aligned} \quad (6.10)$$

are both linear. Such a combination of properties is called *bilinearity*. An equivalent reformulation of bilinearity is the following *distributivity law*:

$$\begin{aligned} &\det(\alpha a + \beta b, \gamma c + \delta d) \\ &= \alpha \gamma \det(a, c) + \alpha \delta \det(a, d) + \beta \gamma \det(b, c) + \beta \delta \det(b, d) \end{aligned} \quad (6.11)$$

for all $a, b, c, d \in \mathbb{K}^2$ and $\alpha, \beta, \gamma, \delta \in \mathbb{K}$.

Example 6.5 (Cramer's Rule in the Coordinate Plane) Any two nonproportional vectors $a, b \in \mathbb{K}^2$ form a *basis* of the coordinate plane in the sense that every vector $v \in \mathbb{K}^2$ admits a unique representation

$$v = x \cdot a + y \cdot b, \text{ where } x, y \in \mathbb{K}. \quad (6.12)$$

Indeed, given such an expression, then in virtue of the relations $\det(a, a) = \det(b, b) = 0$, the evaluation of liner functions (6.10) on the both sides of (6.12) leads to

$$\begin{aligned}\det(v, b) &= \det(x \cdot a + y \cdot b, b) = x \cdot \det(a, b) + y \cdot \det(b, b) = x \cdot \det(a, b), \\ \det(a, v) &= \det(a, x \cdot a + y \cdot b) = x \cdot \det(a, a) + y \cdot \det(a, b) = y \cdot \det(a, b).\end{aligned}$$

Hence, the coefficients x, y in (6.12) are uniquely determined by a, b, v as

$$\begin{aligned}x &= \det(v, b) / \det(a, b), \\ y &= \det(a, v) / \det(a, b).\end{aligned}\tag{6.13}$$

These formulas are known as *Cramer's rule*. To verify that for every $v \in \mathbb{k}^2$, the identity

$$v = \frac{\det(v, b)}{\det(a, b)} \cdot a + \frac{\det(a, v)}{\det(a, b)} \cdot b$$

actually holds, note that the difference $v - \det(v, b) \cdot a / \det(a, b)$ is proportional to b , because

$$\det\left(v - \frac{\det(v, b)}{\det(a, b)} \cdot a, b\right) = \det(v, b) - \frac{\det(v, b)}{\det(a, b)} \cdot \det(a, b) = 0.$$

Therefore, $v = \det(v, b) \cdot a / \det(a, b) + \lambda \cdot b$ for some $\lambda \in \mathbb{k}$. As we have just seen, this forces $\lambda = \det(a, v) / \det(a, b)$.

6.2 Bases and Dimension

6.2.1 Linear Combinations

Let V be an arbitrary module over a commutative ring K with unit. A finite expression of the form $\lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_m w_m$, where $w_i \in V$, $\lambda_i \in K$, is called a *linear combination* of vectors w_1, w_2, \dots, w_m with coefficients $\lambda_1, \lambda_2, \dots, \lambda_m$. A linear combination is *nontrivial* if not all the λ_i are equal to zero. We say that a set of vectors $\Gamma \subset V$ *spans*⁴ V if every vector in V is a linear combination of some vectors $w_1, w_2, \dots, w_m \in \Gamma$. A K -module is *finitely generated* if it is spanned by a finite set of vectors. A set $E \subset V$ is called a *basis* of V if E generates V and each vector $v \in V$ has a unique expansion as a linear combination of vectors from E .

⁴Or *linearly generates*.

Here uniqueness means that an equality between two linear combinations of basic vectors

$$x_1e_1 + x_2e_2 + \cdots + x_ne_n = y_1e_1 + y_2e_2 + \cdots + y_ne_n, \text{ where } e_i \in E, x_i, y_i \in K,$$

forces $x_i = y_i$ for all i . If a K -module V admits a basis $E \subset V$, then V is called a *free K -module*. By definition, every vector v in a free module V with basis E can be uniquely written as a linear combination $v = \sum_{e \in E} x_e e$ in which all but finitely many coefficients $x_e(v)$ vanish. The coefficients $x_e = x_e(v)$ of this expression are called the *coordinates* of v in the basis E .

Caution 6.2 When K is not a field, a K -module will not be free in general. For example, the additive abelian group $\mathbb{Z}/(n)$, considered as a \mathbb{Z} -module,⁵ is generated by the class $[1]_n$, because every class $[m]_n = m \cdot [1]_n$ is proportional to $[1]_n$ with coefficient $m \in \mathbb{Z}$. However, $\mathbb{Z}/(n)$ does not admit a basis over \mathbb{Z} , since for every vector $[m]_n$, two different multiples $\lambda \cdot [m]_n = [\lambda m]_n$ and $\mu \cdot [m]_n = [\mu m]_n$ are equal in $\mathbb{Z}/(n)$ as soon as $\lambda = \mu + kn$ in \mathbb{Z} .

Example 6.6 (Coordinate Module K^n) A coordinate module K^n over an arbitrary commutative ring K with unit is defined in the same way as the coordinate plane from Example 6.4. By definition, a vector of K^n is an ordered collection of n elements⁶ of K arranged in either columns or rows⁷ of size n :

$$(x_1, x_2, \dots, x_n), \quad x_i \in K.$$

Addition of vectors and multiplication of vectors by scalars are defined componentwise:

$$\begin{aligned} (x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) &\stackrel{\text{def}}{=} (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n) \\ \lambda \cdot (x_1, x_2, \dots, x_n) &\stackrel{\text{def}}{=} (\lambda_1, \lambda_2, \dots, \lambda_n)n. \end{aligned}$$

The *standard basis* of K^n consists of the vectors

$$e_i = (0, \dots, 0, 1, 0, \dots, 0), \quad 1 \leq i \leq n, \quad (6.14)$$

where all but the i th coordinates vanish. Clearly,

$$(x_1, x_2, \dots, x_n) = x_1e_1 + x_2e_2 + \cdots + x_ne_n$$

⁵See Example 6.3 on p. 124.

⁶More scientifically, we could say that K^n is a direct product of n copies of the abelian group K equipped with componentwise multiplication by elements $\lambda \in K$.

⁷To save space, we shall usually write them in rows. However, when the column notation becomes more convenient, we shall use it as well.

is the unique expression of the vector $v = (x_1, x_2, \dots, x_n) \in K^n$ as a linear combination of e_1, e_2, \dots, e_n . Thus, K^n is free and admits a basis of cardinality n .

Example 6.7 (Matrices) An $m \times n$ matrix over K is a rectangular array with m rows and n columns,

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

filled by scalars $a_{ij} \in K$. We write $\text{Mat}_{m \times n}(K)$ for the K -module of all $m \times n$ matrices over K . Addition of matrices and multiplication of matrices by scalars are defined componentwise as follows: the (i, j) entry of the linear combination $\lambda A + \mu B$ equals $\lambda a_{ij} + \mu b_{ij}$, where a_{ij}, b_{ij} are the (i, j) entries of the matrices $A = (a_{ij}), B = (b_{ij})$. For example, in $\text{Mat}_{2 \times 3}(\mathbb{Z})$, we have

$$2 \cdot \begin{pmatrix} 1 & 0 & -1 \\ 2 & -1 & 3 \end{pmatrix} - 3 \cdot \begin{pmatrix} -1 & 1 & 0 \\ 3 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 5 & -3 & -2 \\ 5 & -2 & -9 \end{pmatrix}.$$

In particular, the coordinate module K^n can be thought of either as a module of one-row matrices $\text{Mat}_{1 \times n}(K)$ or as a module of one-column matrices $\text{Mat}_{n \times 1}(K)$. We write E_{ij} for a matrix that has 1 in the (i, j) cell and 0 in all the other cells. An arbitrary matrix $A = (a_{ij})$ is uniquely expanded in terms of the E_{ij} as $A = \sum_{ij} a_{ij} E_{ij}$. Thus, the mn matrices E_{ij} form a basis of the module $\text{Mat}_{m \times n}(K)$. They are called the *standard basis matrices*. Thus, the module $\text{Mat}_{m \times n}(K)$ is free and admits a basis of cardinality mn .

Example 6.8 (Module of Functions) For a set X , the ring K^X of all functions $f : X \rightarrow K$ can be considered a K -module with respect to the standard pointwise addition and multiplication by constants

$$f_1 + f_2 : x \mapsto f_1(x) + f_2(x) \quad \text{and} \quad \lambda f : x \mapsto \lambda f(x).$$

For the finite set $X = \{1, 2, \dots, n\}$, there exists an isomorphism of K -modules $K^X \cong K^n$ sending a function $f : X \rightarrow K$ to the collection of its values $(f(1), f(2), \dots, f(n)) \in K^n$. The inverse isomorphism sends the standard basic vector $e_i \in K^n$ to the δ -function $\delta_i : X \rightarrow K$ defined by

$$\delta_i : k \mapsto \begin{cases} 1 & \text{if } k = i \\ 0 & \text{if } k \neq i. \end{cases} \quad (6.15)$$

Example 6.9 (Space of Subsets) Let $K = \mathbb{F}_2 = \{0, 1\}$ be the field of two elements. For a set X , write \mathbb{F}_2^X for the vector space of all functions $\chi : X \rightarrow \mathbb{F}_2$ considered

in Example 6.8 above, and write $\mathcal{S}(X)$ for the set of all subsets of X . There is a natural bijection $\mathcal{S}(X) \simeq X^{\mathbb{F}_2}$ taking a subset $Z \subset X$ to its *characteristic function* $\chi_Z : X \rightarrow \mathbb{F}_2$ defined by

$$\chi_Z(x) = \begin{cases} 1 & \text{for } x \in Z \\ 0 & \text{for } x \notin Z. \end{cases}$$

The inverse map takes a function $\chi_Z : X \rightarrow \mathbb{F}_2$ to its *support* $\text{Supp}(\chi) = \{x \in X \mid \chi(x) \neq 0\}$. The vector space structure on \mathbb{F}_2^X can be transferred to $\mathcal{S}(X)$ by means of this bijection. Then the addition of functions becomes the *symmetric difference* of subsets $Z_1 \triangle Z_2 \stackrel{\text{def}}{=} Z_1 \cup Z_2 \setminus Z_1 \cap Z_2$. Multiplication of functions by 0 and 1 becomes $0 \cdot Z \stackrel{\text{def}}{=} \emptyset$ and $1 \cdot Z \stackrel{\text{def}}{=} Z$ respectively.

Exercise 6.2 By a direct verification of the axioms, check that the operations just defined provide $\mathcal{S}(X)$ with the structure of a vector space over \mathbb{F}_2 . For the finite set $X = \{1, 2, \dots, n\}$, give a basis of $\mathcal{S}(X)$ over \mathbb{F}_2 .

Example 6.10 (Polynomials and Power Series) The polynomial ring $K[x]$ can be considered a K -module with respect to the usual addition of polynomials and multiplication of polynomials by constants. By the definition of $K[x]$, the countable set of the monomials $1, x, x^2, \dots$ is a basis of $K[x]$ over K . The polynomials of degree at most n form a submodule $K[x]_{\leq n} \subset K[x]$, and the monomials $1, x, x^2, \dots, x^n$ form a basis of $K[x]_{\leq n}$.

Exercise 6.3 Show that every collection of monic polynomials f_0, f_1, \dots, f_n such that $\deg f_k = k$ for each k is a basis in $K[x]_{\leq n}$.

The formal power series with coefficients in K also clearly form a K -module. However, in contrast with $K[x]$, the monomials x^m , $m \geq 0$, do not form a basis of $K[[x]]$, because a series with infinitely many nonzero coefficients cannot be written as a finite linear combination of monomials. To find a basis in $K[[x]]$, we have to use the axiom of choice and transfinite machinery.⁸

Exercise 6.4 Show that the vector space $\mathbb{Q}[[x]]$ over \mathbb{Q} does not admit a countable basis.

6.2.2 Linear Dependence

A set of vectors S in a K -module V is said to be *linearly independent* if every nontrivial *linear combination* of the vectors in S does not vanish, i.e., if every

⁸See Sect. 6.2.4 on p. 134.

relation

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m = 0, \text{ where } v_i \in V, \lambda_i \in K, \quad (6.16)$$

forces all the λ_i to be zero. Conversely, a set S is *linearly dependent* or *linearly related* if some nontrivial linear combination of vectors in S equals zero, i.e., the equality (6.16) holds for some $v_i \in S$ and some $\lambda_i \in K$ not all equal to zero. Such an equality (as well as the nontrivial linear combination of vectors v_i on the left-hand side) is called a *linear relation* among v_1, v_2, \dots, v_m . Note that every set of vectors containing the zero vector is linearly related.⁹

A linear expression $v_m = \mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_{m-1} v_{m-1}$ can be rewritten as the linear relation

$$\mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_{m-1} v_{m-1} - v_m = 0.$$

Thus, if some vector in S can be expressed as a linear combination of some other vectors in S , then S is linearly related. For a vector space V over a field \mathbb{k} , the converse is also true: if vectors $v_1, v_2, \dots, v_m \in V$ are linearly related, then one of them is a linear combination of the others. Indeed, the linear relation (6.16) allows us to express any v_i such that $\lambda_i \neq 0$ in terms of the others. For example, if $\lambda_m \neq 0$ in (6.16), then

$$v_m = -\frac{\lambda_1}{\lambda_m} v_1 - \frac{\lambda_2}{\lambda_m} v_2 - \cdots - \frac{\lambda_{m-1}}{\lambda_m} v_{m-1}.$$

In particular, two vectors in a vector space are linearly related if and only if they are proportional.¹⁰

For modules over an arbitrary ring K , the existence of a linear relation (6.16) does not permit us, in general, to express one of the vectors v_i as a linear combination of the others. For example, let $V = K = \mathbb{Q}[x, y]$. The polynomials x and y , considered as vectors in V , are linearly related over K , because $\lambda x - \mu y = 0$ for $\lambda = y, \mu = x$. However, there is no $f \in K$ such that $x = fy$ or $y = fx$.

Lemma 6.1 *Assume that a K -module V is generated by a set $E \subset V$. Then E is a basis of V if and only if E is linearly independent.*

Proof If $\sum \lambda_i e_i = 0$ for some $e_i \in E$ and some $\lambda_i \in K$ not all equal to zero, then the zero vector has two different linear expansions $0 = \sum x_i e_i = \sum 0 \cdot e_i$. Conversely, if $\sum x_i e_i = \sum y_i e_i$, where $x_i \neq y_i$ for some i , then $\sum (x_i - y_i) e_i = 0$ is a nontrivial linear relation among the e_i . \square

⁹Since if $v_1 = 0$, for instance, then we can take $\lambda_1 = 1$ and all the other $\lambda_i = 0$.

¹⁰See Sect. 6.1.3 on p. 125.

6.2.3 Basis of a Vector Space

At this point, we break the discussion of generic K -modules until Chap. 14 and concentrate on the case of vector spaces V over an arbitrary field \mathbb{k} .

Lemma 6.2 (Exchange Lemma) *Assume that the vectors w_1, w_2, \dots, w_m generate the vector space V and that the vectors $u_1, u_2, \dots, u_k \in V$ are linearly independent. Then $m \geq k$, and after appropriate renumbering of the vectors w_i and replacing the first k of them by u_1, u_2, \dots, u_k , the resulting collection*

$$u_1, u_2, \dots, u_k, w_{k+1}, w_{k+2}, \dots, w_m$$

will generate V as well.

Proof Let $u_1 = x_1 w_1 + x_2 w_2 + \dots + x_m w_m$. Since the vectors u_i are linearly independent, we have $u_1 \neq 0$, and therefore, not all the x_i equal zero. Renumber the w_i in order to have $x_1 \neq 0$. Then

$$w_1 = \frac{1}{x_1} u_1 - \frac{x_2}{x_1} w_2 - \dots - \frac{x_m}{x_1} w_m.$$

Therefore, $u_1, w_2, w_3, \dots, w_m$ span V . Now proceed by induction. Assume that for some i in the range $1 \leq i < k$, the vectors $u_1, \dots, u_i, w_{i+1}, \dots, w_m$ span V . Then

$$u_{i+1} = y_1 u_1 + y_2 u_2 + \dots + y_i u_i + x_{i+1} w_{i+1} + x_{i+2} w_{i+2} + \dots + x_m w_m. \quad (6.17)$$

Since the vectors u_i are linearly independent, the vector u_{i+1} cannot be expressed as a linear combination of just the vectors u_1, u_2, \dots, u_i , i.e., there is some $x_{i+j} \neq 0$ in (6.17). Therefore, $m > i$, and we can renumber the vectors w_j in (6.17) in order to have $x_{i+1} \neq 0$. Then the vector w_{i+1} can be expressed as a linear combination of the vectors $u_1, u_2, \dots, u_{i+1}, w_{i+2}, w_{i+3}, \dots, w_m$. Hence, this set of vectors span V . This completes the inductive step of the proof. \square

Exercise 6.5 Show that a vector space V is finitely generated if and only if the cardinalities of all the finite linearly independent subsets of V are bounded above.

Theorem 6.1 *In every vector space V over a field \mathbb{k} , every generating set of vectors contains a basis of V , and every linearly independent set of vectors can be extended to a basis of V . Moreover, all bases of V have the same cardinality.*

Proof We prove the theorem under the additional assumption that V is finitely generated. In the general case, the proof is similar but uses some transfinite arguments. We sketch those arguments in Sect. 6.2.4 below.

By Lemma 6.1, the bases of V are exactly the linearly independent generating sets of vectors. By Lemma 6.2, the cardinality of a linearly independent set is less

than or equal to the cardinality of any generating set. Therefore, all the bases have the same cardinality.

Now let the vectors v_1, v_2, \dots, v_m span V . If they are linearly related, then one of them is a linear combination of the others. If we remove this vector, the remaining set will generate V as well. After a finite number of such removals, we will end up with a linearly independent generating set, that is, a basis of V .

Finally, let the vectors e_1, e_2, \dots, e_k be linearly independent. If they do not span V , then there exists some $v \in V$ that cannot be written as a linear combination of e_1, e_2, \dots, e_k . If we add such a v to e_1, e_2, \dots, e_k , the resulting collection of $k + 1$ vectors will also be linearly independent. Since the cardinalities of linearly independent sets of vectors in a finitely generated vector space are bounded above by [Exercise 6.5](#), after a finite number of such extensions we will have a linearly independent generating set. \square

Definition 6.3 Let V be a vector space over any field \mathbb{k} . The cardinality of any basis in V is called a *dimension* of V and is denoted $\dim V$ or $\dim_{\mathbb{k}} V$, if the precise reference to the ground field is required. Finitely generated vector space is called *finite-dimensional*.

Corollary 6.1 In an n -dimensional vector space V , the following properties of a collection of n vectors are equivalent:

- (1) They are linearly independent.
- (2) They span V .
- (3) They form a basis of V .

Proof Let e_1, e_2, \dots, e_n be a basis in V and v_1, v_2, \dots, v_n the given vectors. If they are linearly independent, then by [Lemma 6.2](#), replacement of all vectors e_i by vectors v_i leads to a generating collection of vectors. Hence, (1) \Rightarrow (2). If the vectors v_i generate V , then by [Theorem 6.1](#), some of them form a basis of V . Since the cardinality of this basis equals n , we conclude that (2) \Rightarrow (3). The implication (3) \Rightarrow (1) was a part of [Lemma 6.1](#). \square

Corollary 6.2 Every n -dimensional vector space V over a field \mathbb{k} is isomorphic to the coordinate space \mathbb{k}^n . The isomorphisms $F : \mathbb{k}^n \xrightarrow{\sim} V$ are in one-to-one correspondence with the bases of V .

Proof For every isomorphism $F : \mathbb{k}^n \xrightarrow{\sim} V$, the images of the standard basis vectors¹¹ $e_i \in \mathbb{k}^n$ form a basis in V . Conversely, for any basis v_1, v_2, \dots, v_n in V , the map

$$F : \mathbb{k}^n \rightarrow V, \quad (x_1, x_2, \dots, x_n) \mapsto x_1 v_1 + x_2 v_2 + \dots + x_n v_n,$$

is linear, bijective, and takes $e_i \in \mathbb{k}^n$ to $v_i \in \mathbb{k}^n$. \square

¹¹See formula (6.14) on p. 128.

Corollary 6.3 Every n -dimensional vector space V over a finite field of cardinality q consists of q^n vectors. \square

Example 6.11 (Finite Field Extensions) Let $\mathbb{k} \subset \mathbb{F}$ be an extension of fields. Then \mathbb{F} is a vector space over \mathbb{k} . If it has finite dimension $\dim_{\mathbb{k}} \mathbb{F} = d$, then the extension $\mathbb{k} \subset \mathbb{F}$ is called a *finite extension of degree d* . In this case, every element $\zeta \in \mathbb{F}$ is algebraic over \mathbb{k} , because an infinite set of powers ζ^k is linearly related, and every linear relation among the powers ζ^k represents a polynomial equation in ζ .

In particular, every finite field \mathbb{F} of characteristic p is a finite extension of the prime subfield $\mathbb{F}_p \subset \mathbb{F}$. Then $|\mathbb{F}| = p^d$, where $d = \dim_{\mathbb{F}_p} \mathbb{F}$, by Corollary 6.3. This is a simple conceptual proof of Corollary 3.4 on p. 64.

Exercise 6.6 Show that \mathbb{F}_{p^n} can be a subfield of \mathbb{F}_{p^m} only if $n \mid m$.

6.2.4 Infinite-Dimensional Vector Spaces

Without the assumption that V is finitely generated, the proof of Theorem 6.1 has to be modified in the spirit of Sect. 1.4.3 on p. 15 as follows. For any two sets of vectors $J \subset S$ such that J is linearly independent, write $\mathcal{I}_J(S)$ for the set of all linearly independent sets I such that $J \subset I \subset S$. The set $\mathcal{I}_J(S)$ is partially ordered by inclusion and complete,¹² because every chain $I_\nu \in \mathcal{I}_J(S)$ has the upper bound $I = \bigcup_\nu I_\nu$.

Exercise 6.7 Check that I is linearly independent.

Hence, thanks to Zorn's lemma, Lemma 1.3 on p. 16, every linearly independent set $J \subset S$ is contained in some maximal linearly independent set $E \subset S$. Since for any vector $s \in S \setminus E$, the set $E \cup \{s\}$ is linearly dependent, there exists a finite linear combination

$$\lambda s + \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_m e_m = 0, \text{ where } \lambda \neq 0 \text{ and } e_i \in E.$$

Therefore, all vectors in S can be expressed as a linear combination of vectors in E . In particular, if S generates V , then E is a basis in V . Hence, for any two sets of vectors $J \subset S$ such that J is linearly independent and S spans V , there exists a basis E of V extending J and contained in S . This proves the first two statements of Theorem 6.1.

¹²See Definition 1.2 on p. 16.

That every base in V has the same cardinality of every other basis follows from the Cantor–Schröder–Bernstein theorem¹³ and the following transfinite extension of Lemma 6.2:

Exercise 6.8 Given two sets of vectors $S, I \subset V$ such that S spans V and I is linearly independent, show that there exists a subset $R \subset S$ of the same cardinality as I such that $I \cup (S \setminus R)$ spans V as well.

6.3 Space of Linear Maps

For every pair of vector spaces U, W , the linear maps¹⁴ $F : U \rightarrow W$ form a vector space in which addition and multiplication by constants are defined by

$$\begin{aligned} F + G : u &\mapsto F(u) + G(u) \\ \lambda F : u &\mapsto \lambda F(u). \end{aligned}$$

The space of linear maps $U \rightarrow W$ is denoted by $\text{Hom}(U, W)$, or by $\text{Hom}_{\mathbb{K}}(U, W)$ when we need a precise reference to the ground field.

6.3.1 Kernel and Image

Proposition 6.1 *Let $F : V \mapsto W$ be a linear map and $K, L \subset V$ two sets of vectors such that K is a basis in $\ker F$ and $K \cup L$ is a basis in V . Then all vectors $w_e = F(e)$, $e \in L$, are distinct, and they form a basis in $\text{im } F$. For finite-dimensional V , this leads to the equality*

$$\dim \ker F + \dim \text{im } F = \dim V. \quad (6.18)$$

Proof Since F sends an arbitrary vector $v = \sum_{f \in K} x_f f + \sum_{e \in L} y_e e \in V$ to

$$F(v) = \sum_{f \in K} x_f F(f) + \sum_{e \in L} y_e F(e) = \sum_{e \in L} y_e w_e,$$

¹³It asserts that if there are injective maps of sets $A \hookrightarrow B$ and $B \hookrightarrow A$, then there is a bijection $A \cong B$.

¹⁴See Sect. 6.1.2 on p. 124.

it follows that the vectors w_e span $\text{im } F$. If there is a linear relation

$$0 = \sum_{e \in L} \lambda_e w_e = F\left(\sum_{e \in L} \lambda_e e\right),$$

then $\sum_{e \in L} \lambda_e e \in \ker F$ is forced to be a linear combination of vectors $f \in K$. Since $L \cup K$ is a linearly independent set, all the λ_e are equal to zero. \square

Corollary 6.4 *The following properties of a linear endomorphism $F : V \rightarrow V$ of a finite-dimensional vector space V are equivalent:*

- (1) F is bijective.
- (2) $\ker F = 0$.
- (3) $\text{im } F = V$.

Proof Properties (2) and (3) are equivalent by the relation (6.18). Since (2) means the injectivity of F , property (1) is equivalent to the simultaneous fulfillment of (2) and (3). \square

6.3.2 Matrix of a Linear Map

Let u_1, u_2, \dots, u_n and w_1, w_2, \dots, w_m be bases in vector spaces U and W respectively. Then every linear map $F : U \rightarrow W$ can be completely described by means of some $m \times n$ matrix as follows. Expand the images of the basis vectors in U through the basis vectors in W as

$$F(u_j) = \sum_{i=1}^m w_i \cdot f_{ij} \quad (6.19)$$

and write the coefficients $f_{ij} \in \mathbb{k}$ as an $m \times n$ matrix whose j th column consists of the m coordinates of the vector $F(u_j)$:

$$\begin{pmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{m1} & f_{m2} & \dots & f_{mn} \end{pmatrix} = (F(u_1), F(u_2), \dots, F(u_n)) \in \text{Mat}_{m \times n}(\mathbb{k}). \quad (6.20)$$

This matrix is called the *matrix of F in the bases $\mathbf{u} = (u_1, u_2, \dots, u_n)$, $\mathbf{w} = (w_1, w_2, \dots, w_m)$* . It depends on the choice of both bases and is denoted by $F_{\mathbf{w}\mathbf{u}} = (f_{ij})$ for short.

Exercise 6.9 Verify that addition of linear maps and multiplication of linear maps by constants corresponds to the addition of their matrices and the multiplication of the matrices by constants as defined in Example 6.7 on p. 129.

$b_i = 0$. The following two corollaries follow immediately from Proposition 6.1 and Corollary 6.4.

Corollary 6.5 *If all b_i in (6.23) are equal to zero, then the solutions x form a vector space of dimension at least $n - m$. In particular, for $n > m$, such a system has nonzero solutions.* \square

Corollary 6.6 (Fredholm Alternative) *If $m = n$ in (6.23), then either the equation $A(x) = b$ has a unique solution x for every $b \in \mathbb{K}^m$ or the homogeneous equation $A(x) = 0$ has a nonzero solution $x \neq 0$.* \square

6.4 Vector Subspaces

6.4.1 Codimension

It follows from Theorem 6.1 on p. 132 that every basis of a subspace $U \subset V$ can be extended to a basis of V . In particular, every subspace U in a finite-dimensional vector space V is finite-dimensional, too, and $\dim U \leq \dim V$. The difference of dimensions

$$\operatorname{codim}_V U \stackrel{\text{def}}{=} \dim V - \dim U$$

is called the *codimension* of the vector subspace $U \subset V$. For example, Proposition 6.1 on p. 135 says that for every linear map F , the codimension of $\ker F$ equals the dimension of $\operatorname{im} F$.

Example 6.13 (Hyperplanes) Vector subspaces of codimension 1 in V are called *hyperplanes*. For example, the kernel of every nonzero linear map $\xi : V \rightarrow \mathbb{K}$ is a hyperplane in V . Indeed, since $\operatorname{im} \xi \subset \mathbb{K}$ is nonzero, it is at least 1-dimensional and therefore coincides with \mathbb{K} . Hence, $\dim \ker \xi = \dim V - \dim \operatorname{im} \xi = \dim V - 1$. For example, given some $\alpha \in \mathbb{K}$, the polynomials $f \in \mathbb{K}[x]$ such that $\deg f \leq n$ and $f(\alpha) = 0$ form a hyperplane in the vector space $\mathbb{K}[x]_{\leq n}$ of all polynomials of degree at most n , because they form the kernel of the evaluation map $\operatorname{ev}_\alpha : \mathbb{K}[x]_{\leq n} \rightarrow \mathbb{K}$, $f \mapsto f(\alpha)$, which is linear in f .

Exercise 6.11 Show that every hyperplane $W \subset V$ is a kernel of some nonzero linear map $\xi : V \rightarrow \mathbb{K}$ determined by W uniquely up to proportionality.

6.4.2 Linear Spans

The intersection of any set of vector subspaces in V is a subspace as well. Hence, for every set of vectors $M \subset V$, there exists the smallest vector subspace containing

M . It is called the *linear span* of M and is denoted by

$$\text{span}(M) = \bigcap_{U \supset M} U. \quad (6.24)$$

More explicitly, $\text{span}(M) \subset V$ can be described as the set of all finite linear combinations of vectors in M . Indeed, such linear combinations form a vector space and belong to every vector subspace containing M .

Exercise 6.12*. Show that $\text{span}(M)$ coincides with the intersection of all hyperplanes containing M .

6.4.3 Sum of Subspaces

The union of vector subspaces is almost never a vector space. For example, the union of the 1-dimensional subspaces spanned by the standard basis vectors e_1 and e_2 in the coordinate plane \mathbb{k}^2 does not contain the sum $e_1 + e_2$.

Exercise 6.13 Show that the union of two vector subspaces is a vector space if and only if one of the subspaces is contained in the other.

For a collection of subspaces $U_v \subset V$, the linear span of their union is called the *sum* of the subspaces U_v and is denoted by $\sum_v U_v \stackrel{\text{def}}{=} \text{span} \bigcup_v U_v$. It consists of all finite sums of vectors $u_v \in U_v$. For example,

$$\begin{aligned} U_1 + U_2 &= \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}, \\ U_1 + U_2 + U_3 &= \{u_1 + u_2 + u_3 \mid u_1 \in U_1, u_2 \in U_2, u_3 \in U_3\}, \\ &\dots \end{aligned}$$

Proposition 6.3 For any two finite-dimensional vector subspaces U, W in an arbitrary vector space V , we have the equality

$$\dim(U) + \dim(W) = \dim(U \cap W) + \dim(U + W).$$

Proof Fix some basis e_1, e_2, \dots, e_k in $U \cap W$ and extend it to bases in U and W by appropriate vectors $u_1, u_2, \dots, u_r \in U$ and $w_1, w_2, \dots, w_s \in W$ respectively. It is enough to check that the vectors $e_1, e_2, \dots, e_k, u_1, u_2, \dots, u_r, w_1, w_2, \dots, w_s$ form a basis in $U + W$. They certainly generate $U + W$. If there exists a linear relation

$$\lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_k e_k + v_1 u_1 + v_2 u_2 + \dots + v_r u_r + \mu_1 w_1 + \mu_2 w_2 + \dots + \mu_s w_s = 0,$$

we can move all the vectors w_1, w_2, \dots, w_s to the right-hand side and get the equality

$$\lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_k e_k + v_1 u_1 + v_2 u_2 + \dots + v_r u_r = -\mu_1 w_1 - \mu_2 w_2 - \dots - \mu_s w_s,$$

whose left-hand side lies in U , whereas the right-hand side lies in W . Thus, both sides are linear expansions of the same vector $v \in U \cap W$ through the bases of U and of W respectively. By the construction of these bases, all coefficients v_i and μ_i must vanish, which means that $v = 0$. Hence, all the λ_i are equal to zero as well. \square

Corollary 6.7 *For any two subspaces U, W of a finite-dimensional vector space V , the inequality*

$$\dim(U \cap W) \geq \dim(U) + \dim(W) - \dim(V)$$

holds. In particular, if $\dim(U) + \dim(W) > \dim V$, then $U \cap W \neq 0$.

Proof This follows at once from Proposition 6.3 and the inequality $\dim(U + W) \leq \dim V$. \square

Corollary 6.8 *The following conditions on finite-dimensional subspaces $U, W \subset V$ are equivalent:*

- (1) $\dim(U + W) = \dim U + \dim W$;
- (2) $U \cap W = 0$;
- (3) *every vector $v \in U + W$ has a unique decomposition $v = u + w$, where $u \in U$, $w \in W$.*

Proof Conditions (1), (2) are equivalent by Proposition 6.3. Let us prove the equivalence of (2) and (3). If there is some nonzero vector $v \in U \cap W$, then $0 + 0 = 0 = v + (-v)$ are two different decompositions of the zero vector as a sum $u + w$, $u \in U$, $w \in W$. Conversely, the equality $u_1 + w_1 = u_2 + w_2$ for $u_1, u_2 \in U$, $w_1, w_2 \in W$ implies the equality $u_1 - u_2 = w_2 - w_1$, in which $u_1 - u_2 \in U$, whereas $w_2 - w_1 \in W$. The condition $U \cap W = 0$ forces the vector $u_1 - u_2 = w_2 - w_1 \in U \cap W$ to be zero. Hence $u_1 = u_2$ and $w_1 = w_2$. \square

6.4.4 Transversal Subspaces

Two subspaces $U, W \subset V$ are said to be *transversal* if they satisfy the conditions from Corollary 6.8 above. A sum of transversal subspaces is called a *direct sum* and is denoted by $U \oplus W$. Transversal subspaces $U, W \subset V$ are called *complementary*, if $U \oplus W = V$. By Corollary 6.8, two subspaces $U, W \subset V$ are complementary if and only if $U \cap W = 0$ and $\dim(U) + \dim(W) = \dim(V)$.

Exercise 6.14 Given a linear map $\xi : V \rightarrow \mathbb{k}$ and a vector $v \in V$ such that $\xi(v) \neq 0$, show that the 1-dimensional subspace $\mathbb{k} \cdot v$ spanned by v is complementary to the hyperplane $\ker \xi$.

More generally, a sum of subspaces $U_1, U_2, \dots, U_n \subset V$ is said to be *direct*, denoted by

$$U_1 \oplus U_2 \oplus \cdots \oplus U_n,$$

if every vector $w \in U_1 + U_2 + \cdots + U_n$ admits a unique expansion $w = u_1 + u_2 + \cdots + u_n$, where $u_i \in U_i$. In other words, a sum of subspaces $U_1, U_2, \dots, U_m \subset V$ is direct if and only if every collection of vectors u_1, u_2, \dots, u_m , $u_i \in U_i$, is linearly independent. For example, the vectors e_1, e_2, \dots, e_n form a basis of V if and only if V decomposes as the direct sum of n 1-dimensional subspaces spanned by the vectors e_i .

Exercise 6.15 Show that a sum of subspaces is direct if and only if each of them is transversal to the sum of all the others.

6.4.5 Direct Sums and Direct Products

Given a family of vector spaces V_v , where v runs through some set X , the direct product of abelian groups¹⁶ $\prod_{v \in X} V_v$ is turned into a vector space by means of componentwise multiplication by scalars. Thus, $\lambda \cdot (u_v) + \mu \cdot (w_v) \stackrel{\text{def}}{=} (\lambda u_v + \mu w_v)$ for any two families $(u_v)_{v \in X}, (w_v)_{v \in X} \in \prod_{v \in X} V_v$. The resulting vector space is called the *direct product* of the vector spaces V_v . The families (v_v) having just a finite number of nonzero elements v_v form a subspace in the direct product. This subspace is denoted by $\bigoplus_v V_v \subset \prod_{v \in X} V_v$ and called the *direct sum* of the vector spaces V_v . For all finite sets of spaces V_1, V_2, \dots, V_n the direct sum is equal to the direct product: $V_1 \oplus V_2 \oplus \cdots \oplus V_n = V_1 \times V_2 \times \cdots \times V_n$.

Exercise 6.16 Let the vector space V be the direct sum of subspaces $U_1, U_2, \dots, U_m \subset V$ in the sense of Sect. 6.4.4. Show that V is isomorphic to the direct sum of spaces U_i considered as abstract standalone vector spaces.

For an infinite set X of vector spaces V_v , the direct sum $\bigoplus V_v$ is a proper subspace in the direct product $\prod V_v$. For example, the direct sum of a countable family of 1-dimensional vector spaces \mathbb{Q} is isomorphic to the space of polynomials $\mathbb{Q}[x]$ and is countable as a set, whereas the direct product of the same family of spaces is isomorphic to the space of formal power series $\mathbb{Q}[[x]]$ and is uncountable.¹⁷

¹⁶See Sect. 2.5 on p. 30.

¹⁷Compare with Example 6.10 on p. 130.

6.5 Affine Spaces

6.5.1 Definition and Examples

Let V be a vector space over a field \mathbb{k} . A set A is called an *affine space* over V if for every vector $v \in V$, a *shift transformation*¹⁸ $\tau_v : A \rightarrow A$ is given such that

$$(1) \tau_0 = \text{Id}_A, \quad (2) \forall v, w \in V, \quad \tau_u \circ \tau_w = \tau_{u+w}, \quad (6.25)$$

$$(3) \forall p, q \in A \exists \text{ unique } v \in V : \tau_v(p) = q. \quad (6.26)$$

The first two conditions (6.25) assert that all the shift transformations τ_v , $v \in V$, form an abelian transformation group¹⁹ of the set A . The elements of this group are in bijection with the vectors $v \in V$. The opposite vectors v and $-v$ correspond to the inverse shift transformations τ_v and $\tau_{-v} = \tau_v^{-1}$. The third condition (6.26) means that each point $q \in A$ can be obtained from an arbitrarily given point $p \in A$ by a *unique* shift transformation τ_v . We write $\vec{p}q$ for the vector producing this transformation. One can think of this vector as an arrow drawn from p to q . It follows from (6.25) that $\vec{p}p = 0$ for all $p \in A$ and $\vec{p}q + \vec{q}r = \vec{p}r$ for all $p, q, r \in A$. This forces $\vec{p}q = -\vec{q}p$.

Exercise 6.17 Prove that $\vec{p}q = \vec{r}s} \iff \vec{p}r = \vec{q}s}$.

A shift transformation τ_v can be thought of as an operation of adding a vector $v \in V$ to the points $p \in A$. For this reason, we often write $p + v$ instead of $\tau_v(p)$.

By definition, the *dimension* of an affine space A associated with a given vector space V is equal to $\dim V$.

Example 6.14 The set of monic polynomials of degree m forms an affine space of dimension m over the vector space $V = \mathbb{k}[x]_{\leq(m-1)}$ of polynomials of degree at most $m - 1$. The shift transformation τ_h , $h \in V$, takes each monic polynomial f to $f + h$. Any two monic polynomials f, g of degree m differ by a polynomial $h = f - g \in V$, which is uniquely determined by f, g .

Example 6.15 The previous example is a particular case of the following situation. For a vector subspace $U \subset V$ and vector $v \in V$, let $A = v + U = \{v + u \mid u \in U\}$ be the shift of U by the vector v . Then A is an affine space associated with U . For $h \in U$, the shift transformation τ_h maps $v + u \mapsto v + u + h$. Any two points $p = v + u$ and $q = v + w$ differ by the vector $\vec{p}q = w - u \in U$, uniquely determined by p, q .

¹⁸Also called a *parallel displacement*.

¹⁹See Sect. 1.3.4 on p. 12.

6.5.2 Affinization and Vectorization

A vector space V produces an affine space $\mathbb{A}(V)$ over V called the *affinization* of V . By definition, the points of $\mathbb{A}(V)$ are the vectors of V . The shift transformation $\tau_w : \mathbb{A}(V) \rightarrow \mathbb{A}(V)$ takes v to $v + w$. One can think of the points in $\mathbb{A}(V)$ as the heads of *radial vectors* $v \in V$ drawn from the *origin*, which is the point corresponding to the zero vector.

Exercise 6.18 Check that properties (6.25), (6.26) are satisfied in $\mathbb{A}(V)$.

We write $\mathbb{A}^n = \mathbb{A}(\mathbb{k}^n)$ for the affinization of the n -dimensional coordinate vector space.

Conversely, every affine space A associated with a vector space V can be *vectorized* as follows. Choose some point $p \in A$, which will be called the *center* of the vectorization or the *origin*, and consider the bijective map

$$\text{vec}_p : A \xrightarrow{\sim} V, \quad q \mapsto \overrightarrow{pq},$$

which sends a point to its radial vector drawn from the origin. This map provides A with a vector space structure transferred from V . The resulting vector space is called the *vectorization of A centered at p* . Note that the vector space structure on A obtained by means of a vectorization depends on the center of vectorization. Two addition operations $A \times A \rightarrow A$ obtained under different choices of the origin are different at least in that they have different neutral elements.

Every collection p, e_1, e_2, \dots, e_n that consists of a point $p \in A$ and a basis e_1, e_2, \dots, e_n of V is called an *affine coordinate system* in A . The coefficients x_i of the linear expansion

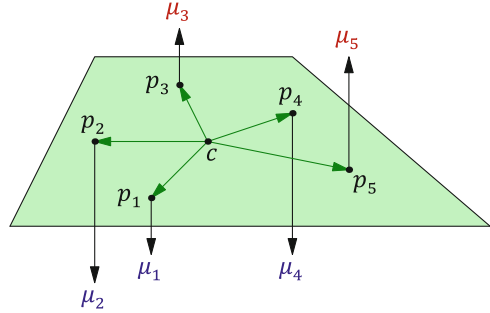
$$\overrightarrow{pq} = x_1 \overrightarrow{pq_1} + x_2 \overrightarrow{pq_2} + \dots + x_n \overrightarrow{pq_n}$$

are called the *affine coordinates* of the point q in the affine coordinate system p, e_1, e_2, \dots, e_n .

6.5.3 Center of Mass

Given a collection of points p_1, p_2, \dots, p_m in an affine space A and a collection of constants $\mu_1, \mu_2, \dots, \mu_m \in \mathbb{k}$ such that $\sum \mu_i \neq 0$, there exists a unique point $c \in A$ such that

$$\mu_1 \overrightarrow{cp_1} + \mu_2 \overrightarrow{cp_2} + \dots + \mu_m \overrightarrow{cp_m} = 0. \quad (6.27)$$

Fig. 6.1 Moments of inertia

Indeed, if we write the linear combination (6.27) for any other point q in the role of c , then the difference between the two sums is

$$\sum \mu_i \vec{q} \vec{p}_i - \sum \mu_i \vec{c} \vec{p}_i = \sum \mu_i \cdot (\vec{q} \vec{p}_i - \vec{c} \vec{p}_i) = \left(\sum \mu_i \right) \cdot \vec{q} \vec{c} = \mu \cdot \vec{q} \vec{c},$$

where $\mu = \sum \mu_i$. Therefore, if q is fixed and c varies through A , the left-hand side of (6.27) vanishes for a unique point c that satisfies $\mu \cdot \vec{q} \vec{c} = \sum \mu_i \vec{q} \vec{p}_i$. We conclude that the point

$$c = q + \frac{\mu_1}{\mu} \cdot \vec{q} \vec{p}_1 + \frac{\mu_2}{\mu} \cdot \vec{q} \vec{p}_2 + \cdots + \frac{\mu_m}{\mu} \cdot \vec{q} \vec{p}_m, \text{ where } \mu = \sum \mu_i, \quad (6.28)$$

is independent of the choice of q and is the only point in A satisfying (6.27). This point c is called the *center of mass*²⁰ for the points $p_1, p_2, \dots, p_m \in A$ taken with masses $\mu_1, \mu_2, \dots, \mu_m \in \mathbb{k}$. The terminology comes from mechanics, where the ground field is $\mathbb{k} = \mathbb{R}$. For the affine space \mathbb{R}^n immersed as a horizontal hyperplane in \mathbb{R}^{n+1} (see Fig. 6.1), the vectors $\vec{c} \vec{p}_i$ are called *moments of inertia* with respect to the point c for the forces μ_i acting at p_i vertically upward if $\mu_i > 0$ and downward if $\mu_i < 0$. The vanishing of the total sum of the moments means that the hyperplane \mathbb{R}^n fastened like a hinge only at the point c remains balanced within \mathbb{R}^{n+1} under the action of all the forces.

In the special case $\mu = \sum \mu_i = 1$, the point c defined in (6.28) is denoted by

$$\mu_1 p_1 + \mu_2 p_2 + \cdots + \mu_m p_m \quad (6.29)$$

and called the *barycenter* of points p_i with weights μ_i . The expression (6.29) is called a *barycentric combination* of the points p_i with weights μ_i . Let me stress that this expression makes sense only for $\sum \mu_i = 1$.

Exercise 6.19 Consider the vectorization $\text{vec}_o : \mathbb{A} \simeq V, q \mapsto \vec{o} \vec{q}$, centered at some point $o \in \mathbb{A}$ and define the point $c \in \mathbb{A}$ by $\vec{o} \vec{c} = \mu_1 \vec{o} \vec{p}_1 + \mu_2 \vec{o} \vec{p}_2 + \cdots + \mu_m \vec{o} \vec{p}_m$. Check that c does not depend on the choice of o if and only if $\sum \mu_i = 1$.

²⁰Or *center of gravity*.

If each point p_i in the barycentric combination (6.29) is a barycentric combination of some other points q_{ij} with weights x_{ij} , i.e., $p_i = \sum_j x_{ij} q_{ij}$, then the barycentric combination (6.29) is simultaneously a barycentric combination of the points q_{ij} , because $\sum_i \mu_i \cdot \sum_j x_{ij} q_{ij} = \sum_{ij} \mu_i x_{ij} q_{ij}$, and new weights $\lambda_{ij} = \mu_i x_{ij}$ have sum 1 as well: $\sum_{ij} \lambda_{ij} = \sum_i \mu_i \cdot \sum_j x_{ij} = \sum_i \mu_i = 1$.

Exercise 6.20 (Mass Grouping Theorem) Consider two collections of points p_i, q_j with weights λ_i, μ_j such that the total weights $\lambda = \sum \lambda_i, \mu = \sum \mu_j$ and their sum $\lambda + \mu$ are nonzero. Write p and q for the centers of mass of the weighted points p_i and q_j respectively. Show that the center of mass of the points p, q with weights λ, μ coincides with the center of mass of the total collection of weighted points²¹ p_i, q_j .

Example 6.16 (Convex Figures in \mathbb{R}^n) Let $\mathbb{k} = \mathbb{R}$, and let \mathbb{A}^n be an affine space over \mathbb{R}^n . A barycentric combination $\sum \lambda_i \cdot p_i$ of points $p_i \in \mathbb{A}^n$ is said to be *convex* if all the λ_i are nonnegative. The set of all convex combinations of two given points a, b is denoted by

$$[pq] \stackrel{\text{def}}{=} \{\lambda p + \mu q \mid \lambda + \mu = 1, \lambda, \mu > 0\}$$

and called the *segment* with endpoints a, b . The set $\Phi \subset \mathbb{A}^n$ is *convex* if every convex combination of every finite collection of points $p_i \in \Phi$ belongs to Φ . For example, every segment $[a, b]$ is convex. Since every finite convex combination can be written as a convex combination of two appropriate points by Exercise 6.20, a set Φ is convex if and only if every segment with endpoints in Φ lies within Φ . The intersection of convex figures is clearly convex. For $M \subset \mathbb{A}^n$, the intersection of all convex sets containing M is called the *convex hull* of M and is denoted by $\text{conv}(M)$. Equivalently, $\text{conv}(M)$ consists of all finite convex barycentric combinations of points in M .

Exercise 6.21 Verify that the set $\text{conv}(M)$ is really convex.

6.5.4 Affine Subspaces

Let A be an affine space over some vector space V . For a given point $p \in A$ and vector subspace $U \subset V$, the set $\Pi(p, U) = p + U = \{\tau_u(p) \mid u \in U\}$ is obviously an affine space over U . It is called the *affine subspace* of dimension $\dim U$ passing through p and *parallel* to U . The subspace U is also called a *direction subspace* of the affine subspace $\Pi(p, U)$.

²¹Each pair of coinciding points $p_i = q_j$ appears in the total collection with weight $\lambda_i + \mu_j$.

Example 6.17 (Lines and Planes) Affine subspaces of dimensions 1 and 2 are called *lines* and *planes*. Therefore, an affine line is nothing but the “trajectory of a free particle,” that is, a locus of points $p + vt$, where $p \in A$ is some “starting” point, $v \in V$ is some nonzero “velocity” vector, and “time” t runs through the ground field \mathbb{k} . Similarly, an affine plane is a locus of points $p + \lambda u + \mu w$, where $p \in A$ is some base point, $u, w \in V$ are some nonproportional vectors, and the coefficients λ, μ run independently through \mathbb{k} . Of course, every line (or plane) has many different such representations depending on the choice of starting points and velocity vectors.

Proposition 6.4 *Let the affine subspaces $\Pi(p, U)$, $\Pi(q, U)$ share the same direction subspace $U \subset V$. Then the following properties are equivalent:*

- (1) $\overrightarrow{pq} \in U$,
- (2) $\Pi(p, U) = \Pi(q, U)$,
- (3) $\Pi(p, U) \cap \Pi(q, U) \neq \emptyset$,
- (4) $p \in \Pi(q, U)$,
- (5) $q \in \Pi(p, U)$.

Proof We first check that (1) \Rightarrow (2). If $\overrightarrow{pq} \in U$, then every point $q + u$, $u \in U$, can be written as $p + w$ for $w = \overrightarrow{pq} + u \in U$. Conversely, every point $p + w$, $w \in U$, can be written as $q + u$ for $u = w - \overrightarrow{pq} \in U$. Hence, $\Pi(p, U) = \Pi(q, U)$. Condition (2) certainly implies (3), (4), (5), and each of conditions (4) and (5) implies (3). Thus, to finish the proof it is enough to show that (3) \Rightarrow (1). Let $r = p + u' = q + u'' \in \Pi(p, U) \cap \Pi(q, U)$, where both $u' = \overrightarrow{pr}$ and $u'' = \overrightarrow{qr}$ belong to U . Then $\overrightarrow{pq} = \overrightarrow{pr} + \overrightarrow{rq} = u' - u'' \in U$. \square

Lemma 6.3 *Given $k + 1$ points p_0, p_1, \dots, p_k in an affine space A over a vector space V , the vectors*

$$\overrightarrow{p_0 p_1}, \overrightarrow{p_0 p_2}, \dots, \overrightarrow{p_0 p_k}$$

are linearly independent in V if and only if the points p_0, p_1, \dots, p_k do not belong to a common affine subspace of dimension less than k in A .

Proof The vectors $\overrightarrow{p_0 p_1}, \overrightarrow{p_0 p_2}, \dots, \overrightarrow{p_0 p_k}$ are linearly related if and only if their linear span has dimension less than k . The latter is equivalent to the existence of a linear subspace $U \subset V$ such that $\dim U < k$ and $\overrightarrow{p_0 p_i} \in U$ for all i . These two conditions say that the affine subspace $p_0 + U$ has dimension less than k and contains all points p_i . \square

Definition 6.4 Points $p_0, p_1, \dots, p_k \in A$ satisfying the conditions from Lemma 6.3 are called *linearly general* or *affinely independent*.

Proposition 6.5 *For any linearly general $k + 1$ points in an affine space A , there exists a unique k -dimensional affine subspace containing these $k + 1$ points. If $\dim A \geq k + 1$, then the converse statement is also true.*

Proof An affine subspace $p_0 + U$ contains all points p_i if and only if all vectors $\overrightarrow{p_0 p_i}$ belong to U . The linear independence of these vectors means that they form

a basis in a k -dimensional vector subspace $U \subset V$ containing them all. Therefore, every such subspace coincides with the linear span of the vectors $\overrightarrow{p_0 p_i}$. Conversely, let the vectors $\overrightarrow{p_0 p_1}, \overrightarrow{p_0 p_2}, \dots, \overrightarrow{p_0 p_k}$ span subspace U of dimension $\ell < k$. Then $n = \dim V \geq \ell + 2$, and there exists a basis e_1, e_2, \dots, e_n in V such that the first ℓ vectors e_1, e_2, \dots, e_ℓ form a basis in U . Write W' and W'' for the linear spans of the vectors²²

$$e_1, \dots, e_\ell, e_{\ell+1}, e_{\ell+3}, \dots, e_{k+1} \quad \text{and} \quad e_1, \dots, e_\ell, e_{\ell+2}, e_{\ell+3}, \dots, e_{k+1}.$$

The affine subspaces $p_0 + W', p_0 + W''$ are distinct and k -dimensional, and each contains all the points p_i . \square

Example 6.18 (Linear Equations: Variation of Example 6.12) Write $U \subset \mathbb{K}^n$ for the linear space of solutions of the homogeneous system of linear equations

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0, \\ a_{31}x_1 + a_{32}x_2 + \dots + a_{3n}x_n = 0, \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0. \end{cases} \quad (6.30)$$

Equivalently, $U = \ker A$, where $A : \mathbb{K}^n \rightarrow \mathbb{K}^m$ is the linear map with matrix $A = (a_{ij})$ in the standard bases of \mathbb{K}^n and \mathbb{K}^m . For a point $p \in \mathbb{A}^n = \mathbb{A}(\mathbb{K}^n)$, the affine subspace $p + U = p + \ker A$ is the set of solutions of the inhomogeneous system of linear equations $A(x) = b$ whose right-hand side is given by $b = A(p) \in \mathbb{K}^m$. This is just another reformulation of the equality $A^{-1}(A(p)) = p + \ker A$ from Proposition 2.1 on p. 32. We conclude again that the solution set of the system

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2, \\ a_{31}x_1 + a_{32}x_2 + \dots + a_{3n}x_n = b_3 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m, \end{cases}$$

either is empty (for $b \notin \text{im } A$) or is an affine subspace in \mathbb{A}^n with direction subspace $U = \ker A$, the solutions of the homogeneous system (6.30).

²²Each collection contains k vectors and is obtained by removing either the vector $e_{\ell+2}$ or the vector $e_{\ell+1}$ from the collection e_1, e_2, \dots, e_{k+1} of $k+1$ vectors.

6.5.5 Affine Maps

Let $\varphi : A \rightarrow B$ be a map of affine spaces A, B associated with vector spaces U, W . Choose an origin $p \in A$ and take $\varphi(p)$ as the origin in B . Then φ induces the map of vectorizations

$$D_p\varphi : U \rightarrow W, \quad \vec{pq} \mapsto \overrightarrow{\varphi(p)\varphi(q)}. \quad (6.31)$$

Lemma 6.4 *If a map (6.31) is linear for some $p \in A$, then it does not depend on the choice of $p \in A$.*

Proof If $D_p\varphi$ is linear, then for every point $r \in A$ and vector $u = \vec{rq} = \vec{pq} - \vec{pr} \in U$,

$$\begin{aligned} D_r\varphi(u) &= \overrightarrow{\varphi(r)\varphi(q)} = \overrightarrow{\varphi(p)\varphi(q)} - \overrightarrow{\varphi(p)\varphi(r)} = D_p\varphi(\vec{pq}) - D_p\varphi(\vec{pr}) \\ &= D_p\varphi(\vec{pq} - \vec{pr}) = D_p\varphi(u). \end{aligned}$$

Therefore $D_r\varphi = D_p\varphi$. □

Definition 6.5 Let A, B be affine spaces associated with vector spaces U, W . A map $\varphi : A \rightarrow B$ is said to be *affine* if the associated map (6.31) is linear and therefore does not depend on p . In this case, the linear map (6.31) is denoted by $D\varphi : U \rightarrow W$ and is called the *differential* of φ .

Proposition 6.6 *Let A, B, C be affine spaces associated with vector spaces U, V, W . For two affine maps $\psi : A \rightarrow B, \varphi : B \rightarrow C$, the composition $\varphi \circ \psi : A \rightarrow C$ is affine, and $D(\varphi \circ \psi) = (D\varphi) \circ (D\psi)$.*

Proof $D_p(\varphi \circ \psi) : \vec{pq} \mapsto \overrightarrow{\varphi\psi(p)\varphi\psi(q)} = D\varphi(\overrightarrow{\psi(p)\psi(q)}) = D\varphi \circ D\psi(\vec{pq})$. □

6.5.6 Affine Groups

It follows from Proposition 6.6 that the bijective affine maps $\varphi : \mathbb{A}(V) \rightarrow \mathbb{A}(V)$ form a transformation group of the affine space $\mathbb{A}(V)$. This group is called the *affine group* of V and is denoted by $\text{Aff}(V)$. It contains the subgroup of shift transformations $\tau_v : p \mapsto p + v$, which are in bijection with the vectors $v \in V$.

Proposition 6.7 *An affine endomorphism $\varphi : \mathbb{A}(V) \rightarrow \mathbb{A}(V)$ is bijective if and only if $D\varphi : V \rightarrow V$ is bijective. An affine automorphism φ is a shift if and only if $D\varphi = \text{Id}_V$.*

Proof Both statements follow from the equality $\varphi(p + v) = \varphi(p) + D\varphi(v)$. □

6.6 Quotient Spaces

6.6.1 Quotient by a Subspace

Let V be a vector space over an arbitrary field \mathbb{k} . Every vector subspace $U \subset V$ provides V with an equivalence relation $v \equiv w \pmod{U}$, meaning that $v - w \in U$, called *congruence modulo U* .

Exercise 6.22 Check that this is really an equivalence relation on V .

We write $[v]_U = v \pmod{U} = v + U = \{w \in V \mid w - v \in U\}$ for the equivalence class of a vector $v \in V$ modulo U . This class coincides with the affine subspace $\Pi(v, U) \subset \mathbb{A}(V)$ parallel to U and passing through $v \in \mathbb{A}(V)$. The congruence classes modulo U form a vector space. Addition and multiplication by scalars are defined by the usual rules

$$[v] + [w] \stackrel{\text{def}}{=} [v + w] \quad \text{and} \quad \lambda[v] \stackrel{\text{def}}{=} [\lambda v].$$

Exercise 6.23 Check that both operations are well defined and satisfy the axioms of a vector space over \mathbb{k} .

The vector space of congruence classes modulo U is denoted by V/U and called the *quotient space* of V by U . The quotient map $\pi : V \twoheadrightarrow V/U, v \mapsto [v]$, is linear and surjective. The vectors of V/U are in bijection with the affine subspaces in $\mathbb{A}(V)$ having U as the direction subspace.

Example 6.19 (Quotient by the Kernel) Associated with a linear map $F : V \rightarrow W$ is a canonical isomorphism

$$V / \ker F \xrightarrow{\sim} \text{im } F, \quad [v] \mapsto F(v). \quad (6.32)$$

Therefore, every linear map $F : V \rightarrow W$ can be decomposed into the quotient epimorphism $V \twoheadrightarrow V / \ker F$ followed by the monomorphism $V / \ker F \simeq \text{im } F \hookrightarrow W$.

Exercise 6.24 Verify that the map (6.32) is well defined, linear, and bijective.

Proposition 6.8 *Let V be a vector space, $U \subset V$ a subspace, and $R \subset U, S \subset V \setminus U$ two sets of vectors such that R is a basis in U and $R \cup S$ is a basis in V . Then the congruence classes $[w]_U, w \in S$, are distinct and form a basis in V/U . For finite-dimensional V , this leads to the equality $\dim(V/U) = \text{codim } U$.*

Proof This follows from Proposition 6.1 on p. 135 applied to the quotient map $V \twoheadrightarrow V/U$. \square

Example 6.20 (Linear Span as a Quotient Space) The linear span

$$W = \text{span}(w_1, w_2, \dots, w_m)$$

of any collection of vectors $w_1, w_2, \dots, w_m \in V$ can be viewed as the image of the linear map $F : \mathbb{k}^m \rightarrow V$ that sends the i th standard basic vector $e_i \in \mathbb{k}^m$ to $w_i \in W$. The kernel of this map $U = \ker F \subset \mathbb{k}^m$ is nothing but the *space of linear relations* among the vectors w_i in V , because it consists of all rows $(\lambda_1, \lambda_2, \dots, \lambda_m) \in \mathbb{k}^m$ such that $\lambda_1 w_1 + \lambda_2 w_2 + \dots + \lambda_m w_m = 0$ in V . The isomorphism $W \simeq \mathbb{k}^m / U$ from Example 6.19 says that the vectors $w \in W$ can be viewed as congruence classes of coordinate rows (x_1, x_2, \dots, x_m) , which encode the linear combinations $x_1 w_1 + x_2 w_2 + \dots + x_m w_m$, modulo those rows that produce the linear relations $\sum x_i w_i = 0$ among the vectors w_i .

6.6.2 Quotient Groups of Abelian Groups

The constructions of quotient space and quotient ring²³ are particular cases of the more general construction of a quotient group. For additive abelian groups, it is described as follows. Let A be an arbitrary abelian group and $B \subset A$ any subgroup. Two elements $a_1, a_2 \in A$ are said to be *congruent modulo B* if $a_1 - a_2 \in B$. This is an equivalence relation on A . We write $a_1 \equiv a_2 \pmod{B}$ for congruent elements and denote by $[a] = a + B$ the congruence class of an element $a \in A$.

Exercise 6.25 Verify that congruence modulo B is an equivalence and the set of congruence classes inherits the abelian group structure, defined by $[a_1] + [a_2] \stackrel{\text{def}}{=} [a_1 + a_2]$.

If besides the abelian group structure, A supports the structure of a K -module, then this K -module structure can be transferred to the quotient group A/B as soon B is a K -submodule of A . In this case, multiplication of a congruence class $[a] \in A/B$ by a constant $\lambda \in K$ is well defined by $\lambda[a] \stackrel{\text{def}}{=} [\lambda a]$.

Exercise 6.26 Check this.

Therefore, for every K -module A and K -submodule B , the quotient module A/B is defined, and the quotient map $A \twoheadrightarrow A/B, a \mapsto [a]_B$, is K -linear. For $A = K$ and B equal to an ideal $I \subset K$, we get a quotient ring K/I . For $K = \mathbb{k}, A = V, B = U \subset V$, we get the quotient space V/U .

²³See Sect. 5.2 on p. 106.

Exercise 6.27 Construct the isomorphism $A/\ker F \xrightarrow{\sim} \operatorname{im} F$ for a K -linear map of K -modules $F : A \rightarrow B$.

Problems for Independent Solution to Chap. 6

Problem 6.1 Prove that the following collections of functions are linearly independent in the space of all functions $\mathbb{R} \rightarrow \mathbb{R}$: (a) $1, \sin x, \sin(2x), \dots, \sin(nx)$,

(b) $1, \sin x, \sin^2 x, \dots, \sin^m x$, (c) $e^{\lambda_1 x}, \dots, e^{\lambda_m x}$, all $\lambda_i \in \mathbb{R}$ distinct,

(d) $x^{\lambda_1}, \dots, x^{\lambda_m}$, all $\lambda_i \in \mathbb{R}$ distinct.

Problem 6.2 Show that \mathbb{R} is an infinite-dimensional vector space over \mathbb{Q} and prove that the following collections of real numbers are linearly independent over \mathbb{Q} :

(a) $\sqrt{2}, \sqrt{3}, \sqrt{5}$, (b) $p_1^{m_1/n_1}, p_2^{m_2/n_2}, \dots, p_s^{m_s/n_s}$, where p_i are distinct prime integers and all m_i/n_i are in $\mathbb{Q} \subset \mathbb{Z}$.

Problem 6.3 Ascertain whether the given collection of functions is linearly independent in the space of all functions $\mathbb{F}_p \rightarrow \mathbb{F}_p$ over the field \mathbb{F}_p :

(a) $1, x, x^2, \dots, x^{p-1}$, (b) x, x^2, \dots, x^p .

Problem 6.4 Find the dimensions of the following vector spaces over \mathbb{Q} :

(a) Polynomials of total degree²⁴ at most d in $\mathbb{Q}[x_1, x_2, \dots, x_m]$.

(b) Homogeneous degree- d polynomials in $\mathbb{Q}[x_1, x_2, \dots, x_m]$.

(c) Homogeneous symmetric²⁵ polynomials of degree 10 in $\mathbb{Q}[x_1, x_2, x_3, x_4]$.

(d) Homogeneous symmetric polynomials of degree at most 3 in $\mathbb{Q}[x_1, x_2, x_3, x_4]$.

Problem 6.5 Let $\zeta \in \mathbb{C} \setminus \mathbb{R}$ be a nonreal complex number, say $\zeta = 3 - 2i$. Find the dimension (over \mathbb{R}) of the space of all polynomials $f \in \mathbb{R}[x]$ such that $\deg f \leq n$ and $f(\zeta) = 0$.

Problem 6.6 Show that the given collection of polynomials forms a basis for the vector space $\mathbb{Q}[x]_{\leq n}$. Write the matrices of the linear maps $D : f(x) \mapsto f'(x)$, $\nabla : f(x) \mapsto f(x) - f(x-1)$, $\Delta : f(x) \mapsto f(x+1) - f(x)$ in the given basis:

(a) $\beta_k(x) = (x+k)^n, 0 \leq k \leq n$,

(b) $\gamma_0(x) = 1$ and $\gamma_k(x) = \binom{x+k}{k} = (x+1) \cdots (x+k)/k!, 1 \leq k \leq n$.

Problem 6.7 For an arbitrary polynomial $q(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in \mathbb{k}[x]$, consider the quotient ring $V = \mathbb{k}[x]/(q)$ as a vector space over \mathbb{k} . Show that a basis in V is formed by the residues $e_\nu = x^\nu \pmod{q}$ for $0 \leq \nu \leq \deg q - 1$

²⁴By definition, the *total degree* of a monomial $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}$ is equal to $\alpha_1 + \alpha_2 + \cdots + \alpha_m$. The total degree of a polynomial f is defined as the maximal total degree of the monomials in f .

²⁵A polynomial $f(x_1, x_2, \dots, x_m)$ is *symmetric* if $f(x_{g_1}, x_{g_2}, \dots, x_{g_m}) = f(x_1, x_2, \dots, x_m)$ for every permutation $g = (g_1, g_2, \dots, g_m) \in S_m$. For example, the polynomial $(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$ is symmetric, whereas the polynomial $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ is not.

and write the matrix of the linear map $F : V \rightarrow V$, $[f] \mapsto [xf]$ in this basis. For $q(x) = (x - \lambda)^n$, where $\lambda \in \mathbb{k}$, find a basis in V in which F has the matrix

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}.$$

Problem 6.8 (Finite Spaces) In an n -dimensional vector space over a finite field of q elements, for each $k = 1, 2, \dots, d$ find the total number of (a) ordered sequences of k linearly independent vectors, (b) k -dimensional vector subspaces. For fixed $k, d \in \mathbb{N}$, write $\binom{d}{k}_q$ for the answer to (b) considered as a function of q . Compute $\lim_{q \rightarrow 1} \binom{d}{k}_q$.

Problem 6.9 Does there exist an inclusion of fields $\mathbb{F}_9 \hookrightarrow \mathbb{F}_{27}$?

Problem 6.10 Let V be a vector space. Suppose the vectors $u_1, u_2, \dots, u_k \in V$ are linearly independent and that the vectors $e_1, e_2, \dots, e_n \in V$ satisfy the following property: for each $i = 1, 2, \dots, k$, the vectors $e_1, \dots, e_{i-1}, u_i, e_{i+1}, \dots, e_n$ form a basis in V . Is it true that for each i , the vectors $u_1, \dots, u_i, e_{i+1}, \dots, e_n$ form a basis of V ?

Problem 6.11 Show that every collection of $n+2$ vectors in an n -dimensional vector space admits a nontrivial linear relation with the sum of the coefficients equal to zero.

Problem 6.12 Give an example of a finite-dimensional vector space W and a triple of mutually transversal subspaces $U, V, T \subset W$ such that $\dim U + \dim V + \dim T = \dim W$ but $W \neq U \oplus V \oplus T$.

Problem 6.13 Let $\dim(U + V) = \dim(U \cap V) + 1$ for some subspaces U, V in a given vector space. Show that $U + V$ equals one of the subspaces U, V and that $U \cap V$ equals the other one.

Problem 6.14 Suppose a collection of k -dimensional subspaces $W_1, W_2, \dots, W_m \subset V$ satisfies the property $\dim W_i \cap W_j = k - 1$ for all $i \neq j$. Show that there exists either a $(k - 1)$ -dimensional subspace $U \subset V$ contained in each of the W_i or a $(k + 1)$ -dimensional subspace $W \subset V$ containing all the W_i .

Problem 6.15 Prove that over an infinite ground field, no finite union of proper vector subspaces exhausts the whole space.

Problem 6.16 Construct the following canonical isomorphisms for an arbitrary triple of vector spaces U, V, W :

- (a) $\text{Hom}(U \oplus W, V) \simeq \text{Hom}(U, V) \oplus \text{Hom}(W, V)$,
- (b) $\text{Hom}(V, U \oplus W) \simeq \text{Hom}(V, U) \oplus \text{Hom}(V, W)$.

Problem 6.17 Let $\dim U = n$, $\dim W = m$. Assume that subspaces $U_0 \subset U$ and $W_0 \subset W$ have dimensions n_0 and m_0 respectively. Show that the set of linear maps

$\{F : U \rightarrow W \mid \ker F \supset U_0 \text{ and } \operatorname{im} F \subset W_0\}$ is a vector subspace in $\operatorname{Hom}(U, W)$ and find its dimension.

Problem 6.18 (Projectors) For a nontrivial idempotent linear endomorphism²⁶ $F : V \rightarrow V$, put $V_0 = \ker F$, $V_1 = \ker(F - \operatorname{Id}_V)$. Show that $V = V_0 \oplus V_1$ and $F(v_0 + v_1) = v_1$ for all $v_0 \in V_0$, $v_1 \in V_1$.

Problem 6.19 (Involutions) For a nontrivial linear involution²⁷ $F : V \rightarrow V$ put

$$V_+ = \{v \in V \mid Fv = v\} = \ker(F - \operatorname{Id}_V),$$

$$V_- = \{v \in V \mid Fv = -v\} = \ker(F + \operatorname{Id}_V).$$

Show that $V_- = \operatorname{im}(F - \operatorname{Id}_V)$, $V_+ = \operatorname{im}(F + \operatorname{Id}_V)$, and $V = V_+ \oplus V_-$.

Problem 6.20 Verify that for every pair of linear endomorphisms $F, G : V \rightarrow V$, one has $\ker(FG) \subset \ker(G)$ and $\operatorname{im}(FG) \subset \operatorname{im}(F)$. Give some finite-dimensional examples for which these inclusions are strict.

Problem 6.21 Prove that for every linear endomorphism $F : V \rightarrow V$ of a finite-dimensional vector space V :

(a) $\ker(F^k) = \ker(F^{k+1}) \Rightarrow \forall n \in \mathbb{N} \ker(F^k) = \ker(F^{k+n})$.

(b) $\operatorname{im}(F^k) = \operatorname{im}(F^{k+1}) \Rightarrow \forall n \in \mathbb{N} \operatorname{im}(F^k) = \operatorname{im}(F^{k+n})$.

(c) $\forall n \in \mathbb{N} \dim \ker(F^n) = \sum_{k=0}^n \dim(\operatorname{im} F^k \cap \ker F)$, where $F^0 \stackrel{\text{def}}{=} \operatorname{Id}_V$.

Problem 6.22 Given a collection of points p_1, p_2, \dots, p_k in an affine space, a segment joining one of the points with the barycenter of all the other points taken with equal weights 1 is called a *median* of the given collection of points. Show that all k medians meet in one point and that this point divides each median in the ratio²⁸ $1 : k$.

Problem 6.23 Given a collection of points p_1, p_2, \dots, p_m in an affine plane \mathbb{A}^2 , is it always possible to choose points q_1, q_2, \dots, q_m such that $p_1, p_2, \dots, p_{m-1}, p_m$ are the midpoints of the respective segments²⁹

$$[q_1, q_2], [q_2, q_3], \dots, [q_{m-1}, q_m], [q_m, q_1]?$$

Problem 6.24 (Barycentric Coordinates) Assume that points $p_0, p_1, \dots, p_n \in \mathbb{A}^n = \mathbb{A}(\mathbb{K}^n)$ do not lie in a common affine hyperplane. Show that the mapping

$$(x_0, x_1, \dots, x_n) \mapsto x_0 p_0 + x_1 p_1 + \dots + x_n p_n$$

establishes a bijection between the collections of weights $(x_0, x_1, \dots, x_n) \in \mathbb{K}^{n+1}$ such that $\sum x_i = 1$ and the points of \mathbb{A}^n . The weights $(\alpha_0, \alpha_1, \dots, \alpha_n)$

²⁶That is, such that $F^2 = F$ but $F \neq 0$ and $F \neq \operatorname{Id}_V$.

²⁷That is, such that $F^2 = \operatorname{Id}_V$ but $F \neq \operatorname{Id}_V$.

²⁸We say that a point c divides the segment $[a, b]$ in the ratio $\alpha : \beta$ if $\beta \cdot \overrightarrow{ca} + \alpha \cdot \overrightarrow{cb} = 0$.

²⁹A point is the *midpoint* of a segment if that point divides the segment in the ratio $1 : 1$.

corresponding to a given point $a \in \mathbb{A}$ are called the *barycentric coordinates* of a with respect to the reference points p_0, p_1, \dots, p_n .

Problem 6.25 For a triple of noncollinear reference points $a, b, c \in \mathbb{A}(\mathbb{R}^2)$, find the barycentric coordinates of the points a_1, b_1, c_1 such that b_1 is the midpoint of $[a, c_1]$, c_1 is the midpoint of $[b, a_1]$, and a_1 is the midpoint of $[c, b_1]$.

Problem 6.26 Given a triple of noncollinear reference points $a, b, c \in \mathbb{A}(\mathbb{R}^2)$, draw the locus of all points p whose barycentric coordinates (α, β, γ) with respect to a, b, c satisfy the following conditions: **(a)** $\alpha, \beta, \gamma > 0$, **(b)** $\alpha, \beta > 0, \gamma < 0$, **(c)** $\alpha = \beta$, **(d)** $\alpha, \beta > 1/3, \gamma > 0$, **(e)** $\alpha \geq \beta$, **(f)** $\alpha \geq \beta \geq \gamma$.

Problem 6.27 Under the conditions of the previous problem, write down some explicit systems of relations among the barycentric coordinates (α, β, γ) defining **(a)** six triangles cut out of Δabc by its medians, **(b)** two triangles obtained from Δabc by homotheties³⁰ with ratios 3 and $1/3$ with the center at the intersection point of the medians of Δabc .

Problem 6.28 Let a linear map $F : V \rightarrow W$ send a subspace $U \subset V$ into a subspace $T \subset W$. Show that the mapping $v \pmod{U} \mapsto F(v) \pmod{T}$ defines a linear map $\tilde{F} : V/U \rightarrow W/T$.

Problem 6.29 For a tower of embedded vector spaces $U \subset V \subset W$, construct a linear embedding $V/U \hookrightarrow W/U$ and an isomorphism

$$(W/U)/(V/U) \simeq W/V.$$

Problem 6.30 For a pair of vector subspaces $U, W \subset V$, construct an isomorphism

$$(U + W)/U \simeq W/(U \cap W).$$

³⁰A homothety with center $c \in \mathbb{A}$ and ratio $\lambda \in \mathbb{k}$ is a map $\gamma_{c,\lambda} : \mathbb{A}^n \rightarrow \mathbb{A}^n, p \mapsto c + \lambda \overrightarrow{cp}$.

Chapter 7

Duality

7.1 Dual Spaces

7.1.1 Covectors

Let V be a vector space over a field \mathbb{k} . A linear map $\xi : V \rightarrow \mathbb{k}$ is called a *covector* or *linear form*¹ on V . The covectors on V form a vector space, denoted by

$$V^* \stackrel{\text{def}}{=} \text{Hom}_{\mathbb{k}}(V, \mathbb{k})$$

and called the *dual space* to V . We have seen in Sect. 6.3.2 on p. 136 that every linear map is uniquely determined by its values on an arbitrarily chosen basis. In particular, every covector $\xi \in V^*$ is uniquely determined by numbers $\xi(e) \in \mathbb{k}$ as e runs through some basis of V . The next lemma is a particular case of Proposition 6.2 on p. 137. However, we rewrite it here once more in notation that does not assume the finite-dimensionality of V .

Lemma 7.1 *Let $E \subset V$ be a basis² of a vector space V . For a linear form $\varphi : V \rightarrow \mathbb{k}$, write $\varphi|_E : E \rightarrow \mathbb{k}$ for the restriction of φ to $E \subset V$. Then the assignment $\varphi \mapsto \varphi|_E$ gives a linear isomorphism between V^* and the space \mathbb{k}^E of all functions $E \rightarrow \mathbb{k}$.*

Exercise 7.1 Verify that the map $\varphi \mapsto \varphi|_E$ is linear.

Proof (of Lemma 7.1) We construct the inverse map $\mathbb{k}^E \rightarrow V^*, f \mapsto \tilde{f}$. For a function $f : E \rightarrow \mathbb{k}$ and vector $v = \sum_{e \in E} x_e e$, put $\tilde{f}(v) = \sum_{e \in E} x_e f(e)$.

¹Also *linear functional*.

²Not necessarily finite.

Exercise 7.2 Verify that both maps $\tilde{f} : V \rightarrow \mathbb{k}$ and $f \mapsto \tilde{f}$ are linear.

Since every linear form $\varphi : V \rightarrow \mathbb{k}$ sends every vector $\sum_{e \in E} x_e e \in V$ to $\varphi\left(\sum_{e \in E} x_e e\right) = \sum_{e \in E} x_e \varphi(e)$, the equalities $\tilde{\varphi}|_E = \varphi$ and $\tilde{f}|_E = f$ hold for all $\varphi \in V^*$ and all $f \in \mathbb{k}^E$. \square

Example 7.1 (Evaluation Functionals) Let $V = \mathbb{k}^X$ be the space of all functions $X \rightarrow \mathbb{k}$ on an arbitrary set³ X . Associated with each point $p \in X$ is the *evaluation functional* $\text{ev}_p : V \rightarrow \mathbb{k}$ sending a function $f : X \rightarrow \mathbb{k}$ to its value $f(p) \in \mathbb{k}$.

Exercise 7.3 Check that $\text{ev}_p : V \rightarrow \mathbb{k}$ is a linear map.

If the set X is finite, then the set of covectors $\{\text{ev}_p\}_{p \in X}$ is a basis in V^* , and the coordinates of every covector $\xi \in V^*$ in this basis are equal to the values of ξ on the delta functions⁴ $\delta_p : X \rightarrow \mathbb{k}$. In other words, every linear form $\xi : V \rightarrow \mathbb{k}$ admits a unique linear expansion through the forms ev_p , and this expansion is

$$\xi = \sum_{p \in X} \xi(\delta_p) \cdot \text{ev}_p. \quad (7.1)$$

Indeed, we know from Example 6.8 on p. 129 that the delta functions form a basis in $V = \mathbb{k}^X$. Therefore, (7.1) holds as soon both sides take equal values on each delta function δ_q . The latter is certainly true, because

$$\text{ev}_p(\delta_q) = \delta_q(p) = \begin{cases} 1 & \text{if } p = q, \\ 0 & \text{otherwise,} \end{cases}$$

by the definition of the delta function. For the same reason, *every* linear expansion $\xi = \sum_{p \in X} \lambda_p \text{ev}_p$, $\lambda_p \in \mathbb{k}$, must have $\lambda_q = \xi(\delta_q)$: just evaluate both sides at δ_q .

Example 7.2 (Coordinate Forms) Let $E \subset V$ be any basis. For each basis vector $e \in E$, write $e^* : V \rightarrow \mathbb{k}$ for the covector taking each vector $v = \sum_{e \in E} x_e e \in V$ to its coordinate $x_e = x_e(v)$ along e . In other words, the set of covectors $\{e^*\}_{e \in E}$ is uniquely defined by the equality $v = \sum_{e \in E} e^*(v) \cdot e$, holding for all $v \in V$.

Exercise 7.4 Check that each map $e^* : V \rightarrow \mathbb{k}$ is linear.

The covectors e^* are called *coordinate forms* of the basis E . In terms of Lemma 7.1, they correspond to delta functions $\delta_e : E \rightarrow \mathbb{k}$; i.e., the values of e^* on the basic vectors $w \in E$ are

$$e^*(w) = \begin{cases} 1 & \text{if } w = e, \\ 0 & \text{if } w \neq e. \end{cases} \quad (7.2)$$

³See Example 6.8 on p. 129.

⁴See formula (6.15) on p. 129.

Proposition 7.1 *For every basis $E \subset V$, the set of coordinate forms $\{e^*\}_{e \in E}$ is linearly independent in V^* . If E is finite, they form a basis of V^* . In particular, $\dim V = \dim V^*$ in this case.*

Proof Evaluation of both sides of the linear relation⁵ $\sum_{e \in E} \lambda_e e^* = 0$ at a basic vector $w \in E$ leads to the equality $\lambda_w = 0$. Therefore, the covectors e^* are linearly independent. If E is finite, then every linear form $\varphi : V \rightarrow \mathbb{k}$ can be linearly expanded through the forms e^* as

$$\varphi = \sum_{e \in E} \varphi(e) \cdot e^*.$$

Indeed, by (7.2), the values of both sides applied to each basic vector $w \in E$ are equal to $\varphi(w)$. \square

Caution 7.1 If a basis E of V is infinite, then the coordinate forms e^* do not span V^* . The restriction isomorphism $V^* \simeq \mathbb{k}^E$ from Lemma 7.1 sends the coordinate form e^* to the delta function $\delta_e : E \rightarrow \mathbb{k}$, whose support is just one point. The linear span of the delta functions consists of all functions $E \rightarrow \mathbb{k}$ with finite support. If E is infinite, the space of all functions is strictly larger. It may have a larger cardinality even as a set. For example, for $\mathbb{k} = \mathbb{Q}$, $E = \mathbb{N}$, the set of finitely supported functions $\mathbb{N} \rightarrow \mathbb{Q}$ is countable, whereas the set of all functions is uncountable.

Example 7.3 (Power Series as Linear Forms on Polynomials) The space of polynomials $\mathbb{k}[x]$ has the standard countable basis formed by monomials x^k . By Lemma 7.1, the dual space $\mathbb{k}[x]^*$ is isomorphic to the space of sequences $f : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{k}$, $f_k = \varphi(x^k)$. The latter are in bijection with their generating power series $f(t) = \sum_{k \geq 0} f_k t^k$. Therefore, $\mathbb{k}[x]^* \simeq \mathbb{k}[[t]]$, and a linear form $\tilde{f} : \mathbb{k}[x] \rightarrow \mathbb{k}$ corresponding to the series

$$f = f_0 + f_1 x + f_2 x^2 + \cdots \in \mathbb{k}[[x]]$$

maps $\tilde{f} : a_0 + a_1 x + \cdots + a_m x^m \mapsto f_0 a_0 + f_1 a_1 + \cdots + f_m a_m$. For example, for every $\alpha \in \mathbb{k}$, the evaluation form $\text{ev}_\alpha : \mathbb{k}[x] \rightarrow \mathbb{k}$, $A(x) \mapsto A(\alpha)$, comes from the power series

$$\sum_{k \geq 0} \alpha^k t^k = (1 - \alpha t)^{-1}.$$

Exercise 7.5 Show that the set of geometric progressions $\{(1 - \alpha t)^{-1}\}_{\alpha \in \mathbb{k}^*}$ is linearly independent in $\mathbb{k}[[t]]$.

In particular, every basis of $\mathbb{R}[t]^*$ over \mathbb{R} should have at least the cardinality of the continuum, whereas $\mathbb{R}[t]$ has a countable basis.

⁵Recall that all but a finite number of the λ_e equal zero.

7.1.2 Canonical Inclusion $V \hookrightarrow V^{**}$

Associated with every vector $v \in V$ is the *evaluation form*

$$\text{ev}_v : V^* \rightarrow \mathbb{k}, \quad \varphi \mapsto \varphi(v),$$

which is a linear form on the dual space V^* , that is, an element of V^{**} . It takes a covector $\varphi \in V^*$ to its value $\varphi(v) \in \mathbb{k}$ on V . Since the latter depends linearly on both v and φ , we get the *canonical*⁶ linear map

$$\text{ev} : V \rightarrow V^{**}, \quad v \mapsto \text{ev}_v. \quad (7.3)$$

Theorem 7.1 *The canonical map (7.3) is injective. If $\dim V < \infty$, then it is an isomorphism. The latter means that every linear form $\xi : V^* \rightarrow \mathbb{k}$ coincides with evaluation $\text{ev}_v : V^* \rightarrow \mathbb{k}$ for some vector $v \in V$ uniquely determined by ξ .*

Proof Injectivity means that for every nonzero vector $v \in V$, there exists some covector $\varphi \in V^*$ such that $\text{ev}_v(\varphi) = \varphi(v) \neq 0$. By Theorem 6.1 on p. 132, the vector v can be included in some basis E of V . Then the coordinate form $\varphi = v^*$ has the required property. If V is of finite dimension, then $\dim V = \dim V^* = \dim V^{**}$ by Proposition 7.1, and therefore, the injective map (7.3) has to be surjective. \square

7.1.3 Dual Bases

The previous theorem says that dual finite-dimensional vector spaces V and V^* are in a completely symmetric relationship with each other.⁷ In particular, each basis $\varphi_1, \varphi_2, \dots, \varphi_n$ in V^* consists of coordinate forms $\varphi_i = e_i^*$ for some basis e_1, e_2, \dots, e_n in V uniquely determined by the basis $\varphi_1, \varphi_2, \dots, \varphi_n$. Namely, the e_i are the vectors whose evaluation forms ev_{e_i} coincide with the coordinate forms φ_i^* of the basis $\varphi_1, \varphi_2, \dots, \varphi_n$ in V^* . Bases $e_1, e_2, \dots, e_n \in V$ and $e_1^*, e_2^*, \dots, e_n^* \in V^*$ are said to be *dual* if each of them consists of the coordinate forms for the other, that is,

$$e_i^*(e_j) = \text{ev}_{e_j}(e_i^*) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

⁶Meaning that it does not depend on any extra data such as the choice of basis.

⁷For infinite-dimensional spaces, this is not true, as we saw in Example 7.3.

Exercise 7.6 Assume that $\dim V = n$ and let $v_1, v_2, \dots, v_n \in V$ and $\varphi_1, \varphi_2, \dots, \varphi_n \in V^*$ satisfy the conditions $\varphi_i(v_i) = 1$ and $\varphi_i(v_j) = 0$ for $i \neq j$. Show that

- (a) Both collections of vectors are bases.
- (b) The i th coordinate of every vector $v \in V$ in the basis v_1, v_2, \dots, v_n is equal to $\varphi_i(v)$.
- (c) The i th coordinate of every covector $\xi \in V^*$ in the basis $\varphi_1, \varphi_2, \dots, \varphi_n$ is equal to $\xi(v_i)$.

Example 7.4 (Lagrange's Formula) Every $n + 1$ distinct constants $a_0, a_1, \dots, a_n \in \mathbb{k}$ produce $n + 1$ evaluation forms on the space $\mathbb{k}[x]_{\leq n}$ of polynomials of degree at most n :

$$\varphi_i = \text{ev}_{a_i} : \mathbb{k}[x]_{\leq n} \rightarrow \mathbb{k}, \quad f \mapsto f(a_i).$$

The polynomial $f_i(x) = \prod_{v \neq i} (x - a_v)$ vanishes at all points a_v except for a_i , where $f_i(a_i) \neq 0$. Therefore, the polynomials $v_i(x) = f_i(x)/f_i(a_i)$ and evaluation forms φ_i satisfy the conditions of [Exercise 7.6](#). Thus, v_i and φ_i form dual bases in $\mathbb{k}[x]_{\leq n}$ and $\mathbb{k}[x]_{\leq n}^*$. This means that each polynomial $g \in \mathbb{k}[x]_{\leq n}$ admits a unique expansion as a linear combination of polynomials $v_i(x)$, and the coefficients of this linear combination equal $g(a_i)$, i.e.,

$$g(x) = \sum_{i=0}^m g(a_i) \cdot v_i(x) = \sum_{i=0}^m g(a_i) \cdot \prod_{v \neq i} \frac{x - a_v}{a_i - a_v}. \quad (7.4)$$

This can be equivalently reformulated as follows. For every collection of constants

$$g_0, g_1, \dots, g_n \in \mathbb{k},$$

there exists a unique polynomial $g \in \mathbb{k}[x]_{\leq n}$ such that $g(a_i) = g_i$ for all i , and this polynomial is given by the formula (7.4), which is known as *Lagrange's interpolation formula*.

Example 7.5 (Taylor's Formula) Assume that $\text{char } \mathbb{k} = 0$, fix some point $a \in \mathbb{k}$, and for $0 \leq k \leq n$ write

$$\varphi_k = \text{ev}_a \circ \frac{d^k}{dx^k} : \mathbb{k}[x]_{\leq n} \rightarrow \mathbb{k}, \quad f \mapsto f^{(k)}(a),$$

for a linear form that sends a polynomial f to the value of its k th derivative $f^{(k)}$ at a , where we put $f^{(0)} \stackrel{\text{def}}{=} f$ to make the notation uniform. The covectors $\varphi_0, \varphi_1, \dots, \varphi_n$ and polynomials $v_k = (x - a)^k/k!$ satisfy the conditions of [Exercise 7.6](#). Hence, they form dual bases in $\mathbb{k}[x]_{\leq n}^*$ and $\mathbb{k}[x]_{\leq n}$. Therefore, every polynomial $g \in \mathbb{k}[x]_{\leq n}$ admits a unique expansion as a linear combination of polynomials $v_i(x)$, and the

coefficients of this linear combination equal $g^{(i)}(a)$:

$$g(x) = g(a) + g'(a) \cdot (x-a) + g''(a) \cdot \frac{(x-a)^2}{2} + \cdots + g^{(n)}(a) \cdot \frac{(x-a)^n}{n!}. \quad (7.5)$$

The expansion (7.5) is called the *Taylor expansion* of g at a . Note that this is an exact equality in $\mathbb{k}[x]$.

7.1.4 Pairings

The symmetry between V and V^* motivates the next helpful notion. Given two vector spaces U, W , a *pairing* between them is a map $\langle *, * \rangle : U \times W \rightarrow \mathbb{k}$ sending each pair of vectors u, w to a number $\langle u, w \rangle \in \mathbb{k}$ that is *bilinear*⁸ in u, w , meaning that for all $v_1, v_2 \in U$, all $w_1, w_2 \in W$, and all $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{k}$, the following equality holds:

$$\begin{aligned} \langle \lambda_1 v_1 + \lambda_2 v_2, \mu_1 w_1 + \mu_2 w_2 \rangle \\ = \lambda_1 \mu_1 \langle v_1, w_1 \rangle + \lambda_1 \mu_2 \langle v_1, w_2 \rangle + \lambda_2 \mu_1 \langle v_2, w_1 \rangle + \lambda_2 \mu_2 \langle v_2, w_2 \rangle. \end{aligned}$$

A pairing is called *perfect* if it possesses the properties listed in Proposition 7.2 below.

Proposition 7.2 (Perfect Pairing) *The following properties of a pairing $\langle *, * \rangle : U \times W \rightarrow \mathbb{k}$ between finite-dimensional vector spaces U, W are equivalent:*

- (1) *For every nonzero $u \in U$, there is some $w \in W$, and for every nonzero $w \in W$, there is some $u \in U$, such that $\langle u, w \rangle \neq 0$.*
- (2) *The map $U \rightarrow W^*$ sending a vector $u \in U$ to the covector $w \mapsto \langle u, w \rangle$ on W is an isomorphism.*
- (3) *The map $W \rightarrow U^*$ sending a vector $w \in W$ to the covector $u \mapsto \langle u, w \rangle$ on U is an isomorphism.*

Proof Since $\langle v, w \rangle$ is bilinear, both maps from (2), (3) are well defined and linear. Condition (1) says that the both are injective. Therefore, if (1) holds, then $\dim U \leq \dim W^*$ and $\dim W \leq \dim U^*$. Since $\dim U = \dim U^*$ and $\dim W = \dim W^*$, both previous inequalities are equalities. This forces both inclusions (2), (3) to be bijective. Thus, (1) implies (2) and (3). Let us show that (2) and (3) are equivalent. By symmetry, it is enough to prove that (2) implies (3). Since (2) forces $\dim U = \dim W$, we have only to check that the map (3) is injective. Let the vector $w_0 \in W$ be in the kernel of map (3). This means that $\langle u, w_0 \rangle = 0$ for all $u \in U$. Since by

⁸See the comments before formula (6.11) on p. 126.

(2), every linear form $\xi : W \rightarrow \mathbb{k}$ maps $\xi(w) = \langle u_\xi, w \rangle$ for appropriate $u_\xi \in U$, we conclude that every linear form $\xi \in W^*$ vanishes at w_0 . This forces $w_0 = 0$.

Exercise 7.7 Verify that for every nonzero vector $w \in W$, there is some covector $\xi \in W^*$ such that $\xi(w) \neq 0$.

Therefore, we get the equivalence (2) \iff (3). The implication (2) & (3) \Rightarrow (1) is obvious. \square

Example 7.6 (Contraction Between Vectors and Covectors) Evaluation of a covector $\varphi \in V^*$ at the vector $v \in V$ gives a perfect pairing

$$\langle v, \varphi \rangle \stackrel{\text{def}}{=} \varphi(v) = \text{ev}_v(\varphi) \quad (7.6)$$

between dual finite-dimensional vector spaces V and V^* . It is called a *contraction* of a vector with a covector. The notation $\langle v, \varphi \rangle$ emphasizes the symmetry between V and V^* , and we will often use it in what follows instead of $\varphi(v)$ or $\text{ev}_v(\varphi)$.

Example 7.7 (2×2 Determinant) A perfect pairing of the coordinate plane \mathbb{k}^2 with itself is defined by the 2×2 determinant⁹

$$\det : \mathbb{k}^2 \times \mathbb{k}^2 \rightarrow \mathbb{k}, \quad (v_1, v_2) \mapsto \det(v_1, v_2).$$

In particular, each linear form $\varphi : \mathbb{k}^2 \rightarrow \mathbb{k}$ can be written as $\varphi(a) = \det(b_\varphi, a)$, where $b_\varphi \in \mathbb{k}^2$ is uniquely determined by φ .

7.2 Annihilators

From this point on, we assume by default that all vector spaces we deal with are finite-dimensional. Every set of covectors $M \subset V^*$ can be viewed as a system of homogeneous linear equations $\{\xi(x) = 0\}_{\xi \in M}$ in the unknown vector $x \in V$. The solution space of this system of equations is denoted by

$$\text{Ann}(M) \stackrel{\text{def}}{=} \{v \in V \mid \forall \xi \in M \ \xi(v) = 0\}$$

and called the *annihilator* of the set $M \subset V^*$. Note that $\text{Ann}(M) \subset V$ is always a vector subspace, because it is the intersection of vector subspaces $\ker \xi$ for all linear forms $\xi : V \rightarrow \mathbb{k}$ from M . Dually, for every set of vectors $N \subset V$, we put $\text{Ann}(N) \stackrel{\text{def}}{=} \{\varphi \in V^* \mid \forall v \in N \ \varphi(v) = 0\}$ and call this subspace the *annihilator* of N . Geometrically, $\text{Ann}(N)$ consists of all hyperplanes in V containing N . Equivalently, one can think of $\text{Ann}(N)$ as the solution space of the system of

⁹See Example 6.4 on p. 125.

homogeneous linear equations $\{e_v(y) = 0\}_{v \in N}$ in the unknown covector $y \in V^*$, that is, the intersection of hyperplanes $\text{Ann}(v) \subset V^*$ taken for all nonzero $v \in N$. Of course, $\text{Ann}(N)$ is a vector subspace in V^* for every set $N \subset V$.

Exercise 7.8 Check that $\text{Ann } N = \text{Ann span } N$ for every subset $N \subset V$.

Proposition 7.3 $\dim U + \dim \text{Ann } U = \dim V$ for every subspace $U \subset V$.

Proof Let the vectors u_1, u_2, \dots, u_k be a basis of U and suppose that the vectors w_1, w_2, \dots, w_m complete them to a basis in V . Therefore, $\dim V = k + m$. Write

$$u_1^*, u_2^*, \dots, u_k^*, w_1^*, w_2^*, \dots, w_m^*$$

for the dual basis of V^* . Then $w_1^*, w_2^*, \dots, w_m^* \in \text{Ann } U$, because for every $v = \sum x_i u_i \in U$,

$$w_v^*(v) = w_v^*(x_1 u_1 + x_2 u_2 + \dots + x_k u_k) = \sum x_i \cdot w_v^*(u_i) = 0.$$

Since every covector $\varphi = \sum y_i u_i^* + \sum z_j w_j^* \in \text{Ann}(U)$ has $y_i = \varphi(u_i) = 0$, the basis covectors $w_1^*, w_2^*, \dots, w_m^*$ span $\text{Ann}(U)$ and therefore form a basis in $\text{Ann}(U)$. Hence, $\dim \text{Ann}(U) = m = \dim V - \dim U$. \square

Corollary 7.1 $\text{Ann Ann}(U) = U$ for every subspace $U \subset V$.

Proof By definition, $U \subset \text{Ann Ann}(U)$. At the same time, Proposition 7.3 implies that $\dim \text{Ann Ann } U = \dim V^* - \dim \text{Ann } U = \dim V^* - \dim V + \dim U = \dim U$. \square

Corollary 7.2 $\dim U + \dim \text{Ann } U = \dim V$ and $\text{Ann Ann}(U) = U$ for every subspace $U \subset V^*$ as well.

Proof Apply Proposition 7.3 and Corollary 7.1 to the dual space V^* instead of V and use the canonical identification $V^{**} \simeq V$. \square

Remark 7.1 In the language of linear equations, the relation $\dim U + \dim \text{Ann } U = \dim V$ means that every vector subspace of codimension m in V can be determined by means of a system of m linearly independent linear homogeneous equations. The dual relation says that conversely, the solution space of every system of m linearly independent linear homogeneous equations has codimension m in V . The equality $\text{Ann Ann}(U) = U$ means that every linear form φ that vanishes on the solution space of linear equations $\{\xi(x) = 0\}_{\xi \in M}$ lies in the linear span of M , i.e., can be linearly expressed through the left-hand sides of the equations.

Exercise 7.9 Show that $\text{Ann Ann } N = \text{span } N$ for every subset $N \subset V$.

Theorem 7.2 *The correspondence $U \leftrightarrow \text{Ann}(U)$ is a bijection between the subspaces of complementary¹⁰ dimensions in V and in V^* . This bijection reverses the inclusions*

$$U \subset W \iff \text{Ann } U \supset \text{Ann } W,$$

and takes the sums of subspaces to the intersections and conversely:

$$\text{Ann} \sum U_i = \bigcap \text{Ann } U_i, \quad \text{Ann} \bigcap U_i = \sum \text{Ann } U_i.$$

Proof Write $\mathcal{S}(V)$ for the set of all vector subspaces in V . The equality $\text{Ann Ann}(U) = U$ means that the maps sending each subspace to its annihilator

$$\begin{array}{ccc} \mathcal{S}(V) & \xrightleftharpoons[\text{Ann } W \mapsto W]{U \mapsto \text{Ann } U} & \mathcal{S}(V^*) \end{array}$$

are inverse to each other. Hence, both are bijective. The implication $U \subset W \Rightarrow \text{Ann } U \supset \text{Ann } W$ is obvious from the definition of annihilator. If we apply this implication to $\text{Ann } W$, $\text{Ann } U$ in the roles of U , W and use equalities $\text{Ann Ann } W = W$, $\text{Ann Ann } U = U$, then we get the opposite implication $\text{Ann } U \supset \text{Ann } W \Rightarrow U \subset W$. The equality

$$\bigcap_v \text{Ann } U_v = \text{Ann} \sum_v U_v \tag{7.7}$$

also follows from the definitions: every linear form annihilating each U_v annihilates the linear span of all U_v and conversely. If we replace U_v by $\text{Ann } U_v$ in (7.7), we get the equality

$$\bigcap_v U_v = \text{Ann} \sum_v \text{Ann } U_v.$$

For the annihilators of the both sides, we get $\text{Ann} \bigcap_v W_v = \sum_v \text{Ann } W_v$. □

Proposition 7.4 *Let V be an arbitrary¹¹ vector space V . For every subspace $U \subset V$, the restriction map*

$$r_U : V^* \rightarrow U^*, \quad \varphi \mapsto \varphi|_U, \tag{7.8}$$

¹⁰That is, between k -dimensional and $(\dim V - k)$ -dimensional subspaces for each $k = 0, 1, \dots, \dim V$.

¹¹Possibly infinite-dimensional.

which takes a linear form $f : V \rightarrow \mathbb{k}$ to its restriction onto $U \subset V$, has $\ker r_U = \text{Ann } U$ and induces a well-defined isomorphism $V^*/\text{Ann } U \xrightarrow{\sim} U^*$, $[\varphi] \mapsto \varphi|_U$. Every linear form $\psi \in \text{Ann } U$ induces a linear form $\overline{\psi} : V/U \rightarrow \mathbb{k}$ well defined by the assignment

$$v \pmod{U} \mapsto \psi(v). \quad (7.9)$$

The resulting map

$$\text{Ann } U \rightarrow (V/U)^*, \quad \psi \mapsto \overline{\psi}, \quad (7.10)$$

is an isomorphism of vector spaces too.

Proof Fix two disjoint sets of vectors $E \subset U$ and $F \subset V$ such that E is a basis of U and $E \sqcup F$ is a basis of V . For every linear form $\xi : U \rightarrow \mathbb{k}$, write $\tilde{\xi} : V \rightarrow \mathbb{k}$ for the linear form that sends each basic vector $e \in E$ to $\xi(e)$ and annihilates all basic vectors $f \in F$. Then $\tilde{\xi}|_U = \xi$. Thus, the linear map (7.8) is surjective. We know from Example 6.19 on p. 149 that r_U induces a well-defined isomorphism $V^*/\text{Ann } U = V^*/\ker r_U \rightarrow \text{im } r_U = U^*$. This proves the first statement. Further, for all $u \in U$, $v \in V$, $\psi \in \text{Ann } U$ we have $\psi(v+u) = \psi(v) + \psi(u) = \psi(v)$. Thus, the covector (7.9) is well defined.

Exercise 7.10 Check that the map (7.10) is linear.

By Proposition 6.8 on p. 149, the congruence classes $[f] = f \pmod{U}$ for $f \in F$ form a basis in V/U . By Lemma 7.1 on p. 155, the covectors $\xi \in (V/U)^*$ are in bijection with functions $F \rightarrow \mathbb{k}$, that is, with collections of constants $\xi_f = \xi([f]) \in \mathbb{k}$. The covectors $\psi \in \text{Ann } U$ also are in bijection with the collections of constants $\psi_f = \psi(f) \in \mathbb{k}$, because of $\psi_e = \psi(e) = 0$ for all $e \in E$. Hence, for every covector $\xi \in (V/U)^*$ there exists a unique covector $\psi \in \text{Ann } U$ such that $\psi(f) = \xi([f])$ for all $f \in F$. The latter means that $\overline{\psi} = \xi$. Therefore, the map (7.10) is bijective. \square

7.3 Dual Linear Maps

7.3.1 Pullback of Linear Forms

Associated with every linear map $F : U \rightarrow W$ is its *dual map* $F^* : W^* \rightarrow U^*$ that sends the linear form $\xi : W \rightarrow \mathbb{k}$ to its composition with F , i.e.,

$$F^*(\xi) = \xi \circ F : u \mapsto \xi(F(u)).$$

Note that F^* acts in the opposite direction to F . For this reason it is often called a *pullback* of linear forms from W to U .

Exercise 7.11 Check that $\varphi \circ F : U \rightarrow \mathbb{k}$ is a linear form bilinearly depending on ξ and F .

Thus, there is well-defined linear dualization map

$$\text{Hom}(U, V) \rightarrow \text{Hom}(W^*, U^*), \quad F \mapsto F^*. \quad (7.11)$$

In more symmetric “contraction notation” from Example 7.6 on p. 161, the dual maps F and F^* are related by the condition

$$\langle v, F^* \xi \rangle = \langle Fv, \xi \rangle \quad \forall \xi \in W^*, v \in V. \quad (7.12)$$

It is obvious from this formula that the canonical identification $V^{**} \cong V$ takes $F^{**} : V^{**} \rightarrow W^{**}$ back to $F : V \rightarrow V$. Thus, the dualization maps $F \mapsto F^*$ and $F^* \mapsto F^{**} = F$ are inverse to each other. In particular, the dualization map (7.11) is an isomorphism of vector spaces.

Exercise 7.12 Show that $(F \circ G)^* = G^* \circ F^*$.

Proposition 7.5 $\ker F^* = \text{Ann im } F$ and $\text{im } F^* = \text{Ann ker } F$.

Proof The first equality follows at once from the definition of F^* written in the form (7.12):

$$\begin{aligned} \xi \in \text{Ann im } F &\iff \forall v \in V \langle Fv, \xi \rangle = 0 \iff \forall v \in V \langle v, F^* \xi \rangle = 0 \\ &\iff F^* \xi = 0. \end{aligned}$$

If we write the first equality for F^* instead of F and take annihilators of both sides, we get the second equality. \square

Corollary 7.3 *Injectivity (respectively surjectivity) of F is equivalent to surjectivity (respectively injectivity) of F^* .* \square

Exercise 7.13 Convince yourself that the two maps described in the statements (2), (3) of Proposition 7.2 on p. 160 are dual to each other and deduce the equivalence (2) \iff (3) from Corollary 7.3.

7.3.2 Rank of a Matrix

Consider two finite-dimensional vector spaces U, W and choose two pairs of dual bases: $\mathbf{u} = (u_1, u_2, \dots, u_m)$, $\mathbf{u}^* = (u_1^*, u_2^*, \dots, u_m^*)$ in U, U^* and $\mathbf{w} = (w_1, w_2, \dots, w_m)$, $\mathbf{w}^* = (w_1^*, w_2^*, \dots, w_m^*)$ in W, W^* . In Sect. 6.3.2 on p. 136, for

is solvable if and only if

$$\operatorname{rk} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \operatorname{rk} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}.$$

Proof The solvability of the system $A(x) = b$ means that the right-hand-side column b lies in the linear span of the columns of the left-hand-side matrix $A = (a_{ij})$. This happens if and only if the attachment of the column b to the matrix A does not change the linear span of the columns. The latter is equivalent to preservation of the dimension of the linear span. \square

Corollary 7.4 *The solutions of a system of homogeneous linear equations*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0, \\ a_{31}x_1 + a_{32}x_2 + \dots + a_{3n}x_n = 0, \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0, \end{cases}$$

form a vector subspace of codimension $\operatorname{rk} A$ in \mathbb{K}^n , where $A = (a_{ij})$ is the matrix of coefficients.

Proof Write $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$ for the linear map with matrix A . Then the solution subspace is nothing but $\ker F$, and $\dim \ker F = n - \dim \operatorname{im} F = n - \operatorname{rk} A$. \square

Problems for Independent Solution to Chap. 7

Problem 7.1 Under the conditions of Example 7.7 on p. 161, find the basis in \mathbb{K}^2 dual to the standard basis $e_1 = (1, 0)$, $e_2 = (0, 1)$ under the pairing $\mathbb{K}^2 \times \mathbb{K}^2 \rightarrow \mathbb{K}$, $(a, b) \mapsto \det(a, b)$. Find the vector $b_\varphi \in \mathbb{K}^2$ corresponding to the linear form $\varphi(x_1, x_2) = x_1 + x_2$ under this pairing.

Problem 7.2 Write $D = \frac{d}{dx} : \mathbb{Q}[x] \rightarrow \mathbb{Q}[x]$ for the differentiation operator $f \mapsto f'$ and consider the polynomial ring¹³ $\mathbb{Q}[D]$. Show that a perfect pairing between¹⁴ $\mathbb{Q}[D]/(D^{n+1})$ and $\mathbb{Q}[x]_{\leq n}$ is well defined by the assignment $(\Phi, f) \mapsto \Phi f(0)$,

¹³It is called the ring of linear differential operators of finite order with constant coefficients.

¹⁴Here $\mathbb{Q}[D]/(D^{n+1})$ means the quotient of the polynomial ring $\mathbb{Q}[D]$ by the principal ideal spanned by D^{n+1} . The vector space $\mathbb{Q}[x]_{\leq n}$ can be thought of as the space of solutions of the linear

which takes $\Phi \in \mathbb{Q}[D]$ and $f \in \mathbb{Q}[x]$ to the constant term of the polynomial¹⁵ Φf . Find the basis in $\mathbb{Q}[D]/(D^{n+1})$ dual to the monomial basis of $\mathbb{Q}[x]_{\leq n}$ under this pairing. Describe the linear endomorphism $D^* \in \text{End}(\mathbb{Q}[D]/(D^{n+1}))$ dual to the differentiation $D \in \text{End}(\mathbb{Q}[x]_{\leq n})$.

Problem 7.3 Show that the matrix $A = (a_{ij}) \in \text{Mat}_{m \times n}(\mathbb{k})$ has rank 1 if and only if $a_{ij} = x_i y_j$ for some nonzero $(x_1, x_2, \dots, x_m) \in \mathbb{k}^m$ and $(y_1, y_2, \dots, y_n) \in \mathbb{k}^n$.

Problem 7.4 Let the matrix $A = (a_{ij}) \in \text{Mat}_{m \times n}(\mathbb{k})$ have $a_{ij} = x_i + y_j$ for some $x_i, y_j \in \mathbb{k}$. Show that $\text{rk } A \leq 2$.

Problem 7.5 Given two matrices $A_1, A_2 \in \text{Mat}_{m \times n}(\mathbb{k})$, let $V_1, V_2 \subset \mathbb{k}^n$ and $W_1, W_2 \subset \mathbb{k}^m$ be the linear spans of their rows and columns respectively. Show that the following conditions are equivalent: (a) $\text{rk}(A_1 + A_2) = \text{rk}(A_1) + \text{rk}(A_2)$, (b) $V_1 \cap V_2 = 0$, (c) $W_1 \cap W_2 = 0$.

Problem 7.6 Show that every matrix of rank r is the sum of at most r matrices of rank 1 and give an example of a rank- r matrix that is not representable as a sum of fewer than r rank-1 matrices.

Problem 7.7 (Commutative Triangle) A diagram of maps between sets is called *commutative* if for every pair of sets X, Y on the diagram every pair of chains of successive maps joining A with B have equal compositions $A \rightarrow B$. For example, the commutativity of the triangle diagram

$$\begin{array}{ccc} A & \xrightarrow{\gamma} & C \\ & \searrow \alpha & \nearrow \beta \\ & B & \end{array}$$

(7.13)

means that $\gamma = \beta \circ \alpha$. Written below are some properties of a commutative triangle (7.13) consisting of abelian groups A, B, C and their homomorphisms α, β, γ . Prove the true properties and disprove the wrong ones by appropriate counterexamples.

- (a) If α and β are surjective, then γ is surjective.
- (b) If α and β are injective, then γ is injective.
- (c) If γ is surjective, then α is surjective.
- (d) If γ is surjective, then β is surjective.
- (e) If γ is injective, then α is injective.
- (f) If γ is injective, then β is injective.
- (g) If α is surjective, then γ is surjective if and only if β is.
- (h) If α is surjective, then γ is injective if and only if β is.

differential equation $D^{n+1}y = 0$ in the unknown function y . Both $\mathbb{Q}[D]/(D^{n+1})$ and $\mathbb{Q}[x]_{\leq n}$ are considered just vector spaces over \mathbb{Q} .

¹⁵Recall that $\Phi f \triangleq a_0 f + a_1 Df + a_2 D^2 f + \dots + a_n D^n f$ for $\Phi = a_0 + a_1 D + \dots + a_n D^n$ (compare with Sect. 4.4 on p. 88).

- (i) If β is surjective, then γ is surjective if and only if α is.
- (j) If β is surjective, then γ is injective if and only if α is.
- (k) If γ is bijective, then α is injective and β is surjective.

Problem 7.8 A chain $\cdots \rightarrow * \rightarrow * \rightarrow * \rightarrow * \rightarrow \cdots$ of homomorphisms of abelian groups is called an *exact sequence* if $\ker \psi = \operatorname{im} \varphi$ for every two consecutive maps $\xrightarrow{\varphi} * \xrightarrow{\psi}$ in the chain. For example, the exactness of the diagrams

$$0 \rightarrow * \xrightarrow{\varphi} *$$

and

$$* \xrightarrow{\psi} * \rightarrow 0$$

means that φ is injective and ψ is surjective. For an exact sequence of vector spaces $0 \rightarrow U \xrightarrow{\varphi} V \xrightarrow{\psi} W \rightarrow 0$ show that the dual diagram $0 \rightarrow W^* \xrightarrow{\psi^*} V^* \xrightarrow{\varphi^*} U^* \rightarrow 0$ is exact as well.

Problem 7.9 For the following commutative diagram of abelian groups with exact rows,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V' & \longrightarrow & V & \longrightarrow & V'' & \longrightarrow & 0 \\ & & \downarrow \varphi' & & \downarrow \varphi & & \downarrow \varphi'' & & \\ 0 & \longrightarrow & W' & \longrightarrow & W & \longrightarrow & W'' & \longrightarrow & 0 \end{array} \quad (7.14)$$

- (a) Show that if φ' and φ'' are isomorphisms, then φ is an isomorphism too.
- (b) Give a counterexample disproving the opposite implication.
- (c) Show that if φ is bijective, then φ' is injective and φ'' is surjective.

Problem 7.10 (Five Lemma) For a commutative diagram of abelian groups with exact rows

$$\begin{array}{ccccccccc} V_1 & \longrightarrow & V_2 & \longrightarrow & V_3 & \longrightarrow & V_4 & \longrightarrow & V_5 \\ \downarrow \varphi_1 & & \downarrow \varphi_2 & & \downarrow \varphi_3 & & \downarrow \varphi_4 & & \downarrow \varphi_5 \\ W_1 & \longrightarrow & W_2 & \longrightarrow & W_3 & \longrightarrow & W_4 & \longrightarrow & W_5 \end{array}$$

where φ_1 is surjective, φ_5 is injective, and both φ_2, φ_4 are bijective, prove that φ_3 is bijective.

Problem 7.11 For a commutative diagram of abelian groups with exact rows

$$\begin{array}{ccccccc}
 0 & \longrightarrow & V' & \longrightarrow & V & \longrightarrow & V'' \longrightarrow 0 \\
 & & & & \downarrow \varphi & & \downarrow \varphi'' \\
 0 & \longrightarrow & W' & \longrightarrow & W & \longrightarrow & W'' \longrightarrow 0
 \end{array}$$

prove that there exists a unique homomorphism $\varphi' : V' \rightarrow W'$ making the left-hand square commutative. Formulate and prove a similar statement for the diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & V' & \longrightarrow & V & \longrightarrow & V'' \longrightarrow 0 \\
 & & \downarrow \varphi' & & \downarrow \varphi & & \\
 0 & \longrightarrow & W' & \longrightarrow & W & \longrightarrow & W'' \longrightarrow 0
 \end{array}$$

Problem 7.12 (Snake Lemma) Given a homomorphism of abelian groups $\varphi : U \rightarrow W$, the quotient group $\text{coker } \varphi \stackrel{\text{def}}{=} W / \text{im } \varphi$ is called the *cokernel* of φ . For the commutative diagram (7.14) with exact rows, construct an exact sequence of homomorphisms

$$0 \rightarrow \ker \varphi' \rightarrow \ker \varphi \rightarrow \ker \varphi'' \rightarrow \text{coker } \varphi' \rightarrow \text{coker } \varphi \rightarrow \text{coker } \varphi'' \rightarrow 0.$$

Problem 7.13 (Eigenvectors and Eigenvalues) Let $F : V \rightarrow V$ be a linear endomorphism of an arbitrary vector space V over a field \mathbb{k} . A nonzero vector $v \in V$ is called an *eigenvector* of F with *eigenvalue* $\lambda \in \mathbb{k}$ if $F(v) = \lambda v$. Prove that:

- (a) Every set of eigenvectors with distinct eigenvalues is linearly independent.
- (b) If every nonzero vector in V is an eigenvector,¹⁶ then $F = \lambda \cdot \text{Id}_V$ for some $\lambda \in \mathbb{k}$.

Problem 7.14 (Nilpotent Endomorphisms) A linear endomorphism $F : V \rightarrow V$ is called *nilpotent* if $F^n = 0$ for some $n \in \mathbb{N}$. For such F , prove that $\ker F \neq 0$, $F^n = 0$ for $n = \dim V$, and all eigenvalues of F equal zero.

Problem 7.15 (Diagonalizable Endomorphisms) A linear endomorphism $F : V \rightarrow V$ is called *diagonalizable* if it has a diagonal matrix¹⁷ in some basis of V . For every such F and subspace $U \subset V$ such that $F(U) \subset U$, prove that the

¹⁶Whose eigenvalue may depend on the vector.

¹⁷A matrix $A = (a_{ij})$ is *diagonal* if $a_{ij} = 0$ for all $i \neq j$.

restriction $F|_U : U \rightarrow U$ is diagonalizable too. Show that the following linear endomorphisms are not diagonalizable:

- (a) Multiplication by the class $[t]$ in the factor ring¹⁸ $\mathbb{k}[t]/(t^n)$ for $n \geq 2$.
- (b) Differentiation $D : f \mapsto f'$ in the space of polynomials of degree at most n for $n \geq 1$.

¹⁸Considered as a vector space over \mathbb{k} .

Chapter 8

Matrices

8.1 Associative Algebras over a Field

8.1.1 Definition of Associative Algebra

A vector space A over a field \mathbb{k} equipped with a multiplication $A \times A \rightarrow A$ is called an *algebra* over the field \mathbb{k} , or just a \mathbb{k} -*algebra* for short, if for every $a \in A$, both the left multiplication map $\lambda_a : A \rightarrow A, v \mapsto av$, and the right multiplication map $\rho_a : A \rightarrow A, v \mapsto va$, are linear. This means that multiplication of vectors by constants commutes with the algebra multiplication: $(\lambda a)b = \lambda(ab) = a(\lambda b)$ for all $\lambda \in \mathbb{k}$ and $a, b \in A$, and the standard distributive law holds for addition and algebra multiplication: $(a_1 + b_1)(a_2 + b_2) = a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2$ for every $a_1, a_2, b_1, b_2 \in A$. An algebra A is called *associative* if $(ab)c = a(bc)$ for all $a, b, c \in A$, and *commutative* if $ab = ba$ for all $a, b \in A$. If there exists $e \in A$ such that $ea = ae = a$ for all $a \in A$, then e is called a *unit*, and we say that A is an *algebra with unit*.

Exercise 8.1 For a \mathbb{k} -algebra A , verify that the unit $e \in A$ is unique (if it exists) and $0 \cdot a = 0$ for all $a \in A$.

Given two \mathbb{k} -algebras A, B , every \mathbb{k} -linear map $\varphi : A \rightarrow B$ such that $\varphi(a_1a_2) = \varphi(a_1)\varphi(a_2)$ for all $a_1, a_2 \in A$ is called a *homomorphism* of \mathbb{k} -algebras.

Basic examples of commutative associative \mathbb{k} -algebras are provided by the polynomial algebra and its factor algebras.¹ The main motivating example of a noncommutative \mathbb{k} -algebra is provided by the algebra of linear endomorphisms of a vector space.

¹See Sect. 5.2.4 on p. 109.

Example 8.1 (Endomorphism Algebra of a Vector Space) The composition of two linear maps $G : U \rightarrow V$, $F : V \rightarrow W$ is linear, because

$$FG(\lambda u + \mu w) = F(\lambda G(u) + \mu G(w)) = \lambda FG(u) + \mu FG(w).$$

Considered as a binary operation, the composition map

$$\text{Hom}(V, W) \times \text{Hom}(U, V) \rightarrow \text{Hom}(U, W), \quad (F, G) \mapsto FG,$$

is bilinear: $(\lambda_1 F_1 + \lambda_2 F_2)G = \lambda_1 F_1 G + \lambda_2 F_2 G$ and $F(\mu_1 G_1 + \mu_2 G_2) = \mu_1 F G_1 + \mu_2 F G_2$. Thus, all linear endomorphisms of a vector space V over a field \mathbb{k} form a \mathbb{k} -algebra $\text{End } V = \text{Hom}(V, V)$ with unit $e = \text{Id}_V$. It is called the *endomorphism algebra* of V . The endomorphism algebra is associative, because both $F(GH)$ and $(FG)H$ map $u \mapsto F(G(H(u)))$.

Exercise 8.2 For a coordinate vector space \mathbb{k}^n , verify that the n^2 linear maps² $E_{ij} : \mathbb{k}^n \rightarrow \mathbb{k}^n$ mapping $e_j \mapsto e_i$ and $e_v \mapsto 0$ for all $v \neq j$ form a basis of $\text{End}(\mathbb{k}^n)$ over \mathbb{k} . Write the multiplication table of these basis maps and show that $\text{End}(\mathbb{k}^n)$ is noncommutative for $\dim V \geq 2$.

8.1.2 Invertible Elements

Given an algebra A with unit $e \in A$, an element $a \in A$ is called *invertible* if there exists $a^{-1} \in A$ such that $aa^{-1} = a^{-1}a = e$. For an associative algebra A , it is enough to demand the existence of $a', a'' \in A$ such that $a'a = aa'' = e$. Then automatically $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$. The same computation shows that a^{-1} is uniquely determined by a in every associative algebra.

Example 8.2 (General Linear Group $\text{GL } V \subset \text{End } V$) By Proposition 1.3, the invertible elements of $\text{End } V$ are the linear isomorphisms $V \xrightarrow{\sim} V$. They form a transformation group³ of V , denoted by $\text{GL } V$ and called the *general linear group* of V .

²Compare with Proposition 6.2 on p. 137.

³See Sect. 1.3.4 on p. 12.

8.1.3 Algebraic and Transcendental Elements

Let A be an associative algebra with unit e over a field \mathbb{k} . Associated with each element $\xi \in A$ is the *evaluation homomorphism*⁴

$$\text{ev}_\xi : \mathbb{k}[t] \rightarrow A, \quad f(x) \mapsto f(\xi) \in A, \quad (8.1)$$

which sends a polynomial $a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m \in \mathbb{k}[x]$ to its value for $x = \xi$ calculated within A , that is, to $a_0\xi^m + a_1\xi^{m-1} + \cdots + a_{m-1}\xi + a_me \in A$. Note that the constant term $a_m = a_m \cdot x^0$ evaluates to $a_m\xi^0 \stackrel{\text{def}}{=} a_me \in A$ by definition.

An element $\xi \in A$ is called *transcendental* over \mathbb{k} if the evaluation homomorphism (8.1) is injective. Equivalently, the transcendence of ξ over \mathbb{k} means that all nonnegative integer powers ξ^m are linearly independent over \mathbb{k} .

An element $\xi \in A$ is called *algebraic* over \mathbb{k} if the evaluation homomorphism (8.1) has nonzero kernel. In this case, $\ker \text{ev}_\xi = (\mu_\xi)$ is the principal ideal⁵ generated by some monic polynomial $\mu_\xi \in \mathbb{k}[x]$, which is uniquely determined by ξ as the monic polynomial of minimal positive degree such that $\mu_\xi(\xi) = 0$. The polynomial μ_ξ is called the *minimal polynomial* of ξ over \mathbb{k} . Note that every polynomial $f \in \mathbb{k}[x]$ such that $f(\xi) = 0$ is divisible by μ_ξ . Equivalently, the algebraicity of ξ over \mathbb{k} means the existence of a nontrivial linear relation between nonnegative integer powers ξ^m . In particular, if a \mathbb{k} -algebra A is of finite dimension over \mathbb{k} , then all its elements $a \in A$ are algebraic over \mathbb{k} .

Example 8.3 (Algebraicity of Linear Endomorphisms) Since $\dim_{\mathbb{k}} \text{End}(V) = n^2$, the iterations $F^0, F^1, F^2, \dots, F^{n^2}$ of a linear endomorphism $F \in \text{End}(V)$ are linearly related. Therefore, F satisfies some polynomial equation of degree at most n^2 . In Sect. 9.6.3 on p. 222 we will show⁶ that F can actually be annihilated by an appropriate polynomial of degree n .

8.2 Matrix Algebras

8.2.1 Multiplication of Matrices

Consider a triple of coordinate vector spaces $\mathbb{k}^n, \mathbb{k}^s, \mathbb{k}^m$ and write

$$u_1, u_2, \dots, u_n \in \mathbb{k}^n, \quad v_1, v_2, \dots, v_s \in \mathbb{k}^s, \quad w_1, w_2, \dots, w_m \in \mathbb{k}^m$$

⁴Compare with Sect. 3.4.2 on p. 54.

⁵Recall that $\mathbb{k}[x]$ is a principal ideal domain. See Sect. 5.3 on p. 109 for the common properties of such rings.

⁶See also Example 8.4 below.

for their standard bases. Assume that linear maps $B : \mathbb{K}^n \rightarrow \mathbb{K}^s$ and $A : \mathbb{K}^s \rightarrow \mathbb{K}^m$ have matrices $A = (a_{ij})$ and $B = (b_{ij})$ in these bases. Then the matrix $P = (p_{ij})$ of their composition

$$P = AB : \mathbb{K}^n \rightarrow \mathbb{K}^m$$

is called the *product of matrices*⁷ A and B . Thus, we get a product defined for every ordered pair of matrices such that the width of the left matrix equals the height of the right. The height of the product is the height of the left factor, and the width of the product is the width of the right factor. The element p_{ij} in the i th row and j th column of the product is equal to the coefficient of w_i in the expansion

$$AB(u_j) = A\left(\sum_k v_k b_{kj}\right) = \sum_k A(v_k) b_{kj} = \sum_i \sum_k w_i a_{ik} b_{kj}.$$

Therefore, $p_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{is}b_{sj}$. This multiplication rule can be reformulated in several equivalent ways suitable for different kinds of practical computations. First of all, one row and one column of the same size s are multiplied as

$$(a_1, a_2, \dots, a_s) \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix} = a_1 b_1 + a_2 b_2 + \cdots + a_s b_s.$$

The result can be viewed either as a linear combination of the a_i with coefficients b_i , or symmetrically as a linear combination of the b_i with coefficients a_i . For a matrix A formed by m rows of size s and a matrix B formed by n columns of size s , the product $P = AB$ has m rows and n columns, and the (i, j) member of P is the product of the i th row of A and the j th column of B :

$$p_{ij} = (a_{i1}, a_{i2}, \dots, a_{is}) \cdot \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{sj} \end{pmatrix}. \quad (8.2)$$

This means that the j th column of AB is a linear combination of s columns⁸ of A with coefficients taken from the j th column of B . For example, if we wish to transform

⁷Note that the order of multipliers in the product of matrices is the same as in the composition of the corresponding linear maps.

⁸Considered as vectors in \mathbb{K}^m .

the matrix

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{pmatrix} \quad (8.3)$$

to the matrix C' such that

- the first column of C' is the sum of the first column of C and the second column of C multiplied by λ ,
- the second column of C' is the sum of the first and third columns of C ,
- the third column of C' is the sum of the third column of C and the second column of C multiplied by μ ,
- C' gets an extra fourth column equal to the sum of each of the columns of C multiplied by its column number,

then we have to multiply C from the right side by the matrix

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ \lambda & 0 & \mu & 2 \\ 0 & 1 & 1 & 3 \end{pmatrix}.$$

Exercise 8.3 Verify this by explicit computation of all matrix elements by formula (8.2).

Symmetrically, the i th row of AB is a linear combination of s rows⁹ of the matrix B with its coefficients taken from the i th row of A . For example, if we would like to transform the same matrix (8.3) to the matrix C'' such that

- the first row of C'' is the second row of C ,
- the second row of C'' is the sum of the second row of C and the first row of C multiplied by λ ,

then we have to multiply C from the left by the matrix $\begin{pmatrix} 0 & 1 \\ \lambda & 1 \end{pmatrix}$.

Exercise 8.4 Verify this in two ways: using the previous description of the columns of the product and via straightforward computation of all elements by formula (8.2).

Comparison of the row-description and the column-description for the product AB leads to the conclusion that the transposition¹⁰ of matrices interacts with the multiplication by the rule

$$(AB)^t = B^t A^t. \quad (8.4)$$

⁹Considered as vectors in \mathbb{k}^n .

¹⁰See Sect. 7.3.2 on p. 165.

Therefore, the transposition map $C \mapsto C^t$ is an *antiautomorphism* of matrix algebras, meaning that it sends a product to the product taken in reverse order.

Exercise 8.5 Verify the equality (8.4) by explicit computation of all matrix elements by the formula (8.2).

Since the composition of linear maps is associative and bilinear, the product of matrices inherits the same properties, that is, $(FG)H = F(GH)$ for all $F \in \text{Mat}_{m \times k}$, $G \in \text{Mat}_{k \times \ell}$, $H \in \text{Mat}_{\ell \times n}$, and

$$\begin{aligned} & (\lambda_1 F_1 + \mu_1 G_1)(\lambda_2 F_2 + \mu_2 G_2) \\ &= \lambda_1 \lambda_2 F_1 F_2 + \lambda_1 \mu_2 F_1 G_2 + \mu_1 \lambda_2 G_1 F_2 + \mu_1 \mu_2 G_1 G_2 \end{aligned}$$

for all $F_i, G_i \in \text{Mat}_{m \times k}(\mathbb{K})$, $\lambda_i, \mu_i \in \mathbb{K}$. Hence the square matrices of size $n \times n$ form an associative \mathbb{K} -algebra with unit

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

(the ones on the main diagonal are the only nonzero matrix elements). This algebra is denoted by

$$\text{Mat}_n(\mathbb{K}) \stackrel{\text{def}}{=} \text{Mat}_{n \times n}(\mathbb{K}) \simeq \text{End}(\mathbb{K}^n).$$

For $n \geq 2$, the algebra $\text{Mat}_n(\mathbb{K})$ is noncommutative. For example,

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 12 & 15 \end{pmatrix} \quad \text{but} \quad \begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 4 & 23 \end{pmatrix}.$$

Example 8.4 (Annihilating Polynomial of a 2×2 Matrix) Let us show that every 2×2 matrix satisfies a quadratic equation:

$$F = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad F^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{pmatrix} = \begin{pmatrix} a^2 + bc & b(a + d) \\ c(a + d) & cb + d^2 \end{pmatrix}$$

can be combined to

$$\begin{aligned} F^2 - (a + d) \cdot F &= \begin{pmatrix} a^2 + bc & b(a + d) \\ c(a + d) & cb + d^2 \end{pmatrix} - \begin{pmatrix} a(a + d) & b(a + d) \\ c(a + d) & d(a + d) \end{pmatrix} \\ &= \begin{pmatrix} (bc - ad) & 0 \\ 0 & (bc - ad) \end{pmatrix} = (bc - ad) \cdot E. \end{aligned}$$

Therefore, F satisfies the equation $F^2 - (a + b)F + (ad - bc)E = 0$. The quantities

$$\det F \stackrel{\text{def}}{=} ad - bc \quad \text{and} \quad \text{tr} F \stackrel{\text{def}}{=} a + b$$

are called the *determinant*¹¹ and *trace* of the matrix F respectively. In terms of the trace and determinant, the quadratic equation on F takes the form

$$F^2 - \text{tr}(F) \cdot F + \det(F) \cdot E = 0. \quad (8.5)$$

8.2.2 Invertible Matrices

The invertible elements of the matrix algebra $\text{Mat}_n(\mathbb{k})$ are exactly the matrices of linear automorphisms of the coordinate space \mathbb{k}^n . They form a transformation group of \mathbb{k}^n , denoted by $\text{GL}_n(\mathbb{k})$ and called the *general linear group* in dimension n over \mathbb{k} .

Example 8.5 (Invertible 2×2 Matrices) It follows from (8.5) that for every $F \in \text{Mat}_2(\mathbb{k})$, the equality

$$\det(F) \cdot E = \text{tr}(F) \cdot F - F^2 = F \cdot (\text{tr}(F)E - F)$$

holds. Assume that $F = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible and multiply both sides by F^{-1} :

$$\det(F) \cdot F^{-1} = \text{tr}(F) \cdot E - F = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \quad (8.6)$$

This forces $\det F$ to be nonzero, because otherwise, we would get the zero matrix on the left-hand side and therefore $a = b = c = d = 0$ on the right; this is impossible for an invertible map F . Thus, every invertible matrix F necessarily has $\det F \neq 0$, and the formula (8.6) gives an explicit expression for F^{-1} :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \quad (8.7)$$

Exercise 8.6 Verify this by the straightforward computation of both products FF^{-1} and $F^{-1}F$.

¹¹See Example 6.4 on p. 125.

8.3 Transition Matrices

Let a vector v be a linear combination of vectors w_1, w_2, \dots, w_m :

$$v = \sum_{i=1}^m x_i w_i = w_1 x_1 + w_2 x_2 + \cdots + w_m x_m. \quad (8.8)$$

If we organize the coefficients $x_i \in \mathbb{k}$ in the column matrix

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} \quad (8.9)$$

and write vectors w_i in the row matrix¹² $\mathbf{w} = (w_1, w_2, \dots, w_m)$, then (8.8) turns into the matrix equality $\mathbf{v} = \mathbf{w}x$, where \mathbf{v} is a 1×1 matrix with its element in V . Such matrix notation makes linear expansions of vectors more compact and transparent, especially when we deal with (numbered) collections of vectors such as bases and generating systems. For two collections of vectors $\mathbf{u} = (u_1, u_2, \dots, u_n)$ and $\mathbf{w} = (w_1, w_2, \dots, w_m)$ such that each vector u_j is linearly expressed through (w_1, w_2, \dots, w_m) as

$$u_j = \sum_{v=1}^m c_{vj} w_v = w_1 \cdot c_{1j} + w_2 \cdot c_{2j} + \cdots + w_m \cdot c_{mj},$$

all these expansions are combined into the single matrix equality $\mathbf{u} = \mathbf{w} \cdot C_{\mathbf{w}\mathbf{u}}$, where the matrix

$$C_{\mathbf{w}\mathbf{u}} = (c_{ij}) = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix} \quad (8.10)$$

is constructed from \mathbf{u} via replacement of each vector u_j by the column of coefficients belonging to its linear expression through (w_1, w_2, \dots, w_m) . The matrix (8.10) is called the *transition matrix* from \mathbf{u} to \mathbf{w} . A particular example of the transition matrix $x = C_{\mathbf{u}\mathbf{v}}$ is the column (8.9) formed by the coefficients of the linear expression of one vector v through the vectors \mathbf{u} .

¹²Note that the elements of this matrix are *vectors*.

If vectors $\mathbf{v} = (v_1, v_2, \dots, v_s)$ are linearly expressed through vectors \mathbf{u} as $\mathbf{v} = \mathbf{u}C_{uv}$, then the transition matrix C_{uw} allows us to express the vectors \mathbf{v} through \mathbf{w} as $\mathbf{v} = \mathbf{w}C_{wu}C_{uv}$. Therefore, the transition matrix from \mathbf{v} to \mathbf{w} is the product of the transition matrices from \mathbf{u} to \mathbf{w} and from \mathbf{v} to \mathbf{u} :

$$C_{wu}C_{uv} = C_{wv}. \quad (8.11)$$

Remark 8.1 If vectors $\mathbf{e} = (e_1, e_2, \dots, e_n)$ are linearly independent, then the transition matrix C_{ew} from any collection of vectors $\mathbf{w} = (w_1, w_2, \dots, w_m)$ to \mathbf{e} is uniquely determined by \mathbf{e} and \mathbf{w} , meaning that two collections of vectors \mathbf{u} , \mathbf{w} coincide if and only if $C_{eu} = C_{ew}$. If there are some nontrivial linear relations between vectors $\mathbf{w} = (w_1, w_2, \dots, w_m)$, then every vector v in the linear span of \mathbf{w} allows many *different* linear expressions¹³ through \mathbf{w} . Therefore, the notation C_{wv} is not correct in this case, because the matrix C_{wv} is not uniquely determined by \mathbf{w} and \mathbf{v} : different matrices may produce the same collection \mathbf{v} . Nevertheless, equality (8.11) is still intentional, and says that given *some* linear expressions C_{wu} , C_{uv} of vectors \mathbf{u} , \mathbf{v} through the vectors \mathbf{v} , \mathbf{w} respectively, their matrix product $C_{wu} \cdot C_{uv}$ gives *some* linear expression C_{wv} of \mathbf{u} through \mathbf{w} .

Lemma 8.1 *Let a collection of vectors $\mathbf{v} = (v_1, v_2, \dots, v_n)$ be a basis of V . Then the collection $\mathbf{u} = \mathbf{v}C_{vu}$ is a basis of V if and only if the transition matrix C_{vu} is invertible. In this case, $C_{vu}^{-1} = C_{uv}$.*

Proof If \mathbf{u} is a basis, then the vectors \mathbf{e} are linearly expressed through \mathbf{u} . It follows from (8.11) that $C_{ee} = C_{eu}C_{ue}$ and $C_{uu} = C_{ue}C_{eu}$. Since the transition matrix from a collection of vectors to a basis is uniquely determined by the collection, we conclude that $C_{ee} = C_{uu} = E$. Hence, the transition matrices C_{ue} and C_{eu} are inverse to each other. If vectors \mathbf{u} are linearly related, say $\mathbf{u}\lambda = 0$ for some nonzero column of constants λ , then $\mathbf{e}C_{eu}\lambda = 0$. Hence, $C_{eu}\lambda = 0$. This matrix equality prevents C_{eu} from being invertible, because otherwise, multiplication of both sides by C_{eu}^{-1} would give $\lambda = 0$. \square

Example 8.6 (Basis Change Effect on Coordinates of Vectors) If the vectors $\mathbf{w} = (w_1, w_2, \dots, w_m)$ are expressed through the basis $\mathbf{e} = (e_1, e_2, \dots, e_n)$ as $\mathbf{w} = \mathbf{e}C_{ew}$ and the vectors $\mathbf{v} = \mathbf{e}C_{ev}$ form another basis, then the transition matrix from \mathbf{w} to \mathbf{v} is

$$C_{vw} = C_{ve}C_{ew} = C_{ev}^{-1}C_{vw}.$$

In particular, the coordinate columns x_e, x_v of the same vector $v \in V$ in the bases \mathbf{e} , \mathbf{v} are related as $x_v = C_{ve} \cdot x_e = C_{ev}^{-1} \cdot x_e$.

Example 8.7 (Basis Change Effect on Matrices of Linear Maps) For every linear map $F : U \rightarrow W$ and collection of vectors $\mathbf{v} = (v_1, v_2, \dots, v_r)$, let us write $F(\mathbf{v})$ for

¹³In Sect. 8.4 we have seen that these linear expansions form an affine subspace in \mathbb{k}^m parallel to the vector subspace of all linear relations on w_1, w_2, \dots, w_m .

the collection $(F(v_1), F(v_2), \dots, F(v_r))$ considered as a row matrix with elements in W . Since F is linear, it follows that for every matrix $M \in \text{Mat}_{r \times s}(\mathbb{K})$, the equality $F(vM) = F(v)M$ holds.

Exercise 8.7 Verify this equality.

For every pair of bases \mathbf{u}, \mathbf{w} in U, W , the matrix F_{wu} of a linear map F in these bases is defined by the assignment¹⁴ $F(\mathbf{u}) = \mathbf{w}F_{wu}$. For another pair of bases $\tilde{\mathbf{u}} = \mathbf{u}C_{u\tilde{u}}$ and $\tilde{\mathbf{w}} = \mathbf{w}C_{w\tilde{w}}$, the matrix of F is

$$F_{\tilde{w}\tilde{u}} = C_{w\tilde{w}}^{-1} F_{wu} C_{u\tilde{u}}, \quad (8.12)$$

because

$$F(\tilde{\mathbf{u}}) = F(\mathbf{u}C_{u\tilde{u}}) = F(\mathbf{u})C_{u\tilde{u}} = \mathbf{w}F_{wu}C_{u\tilde{u}} = \tilde{\mathbf{w}}C_{w\tilde{w}}F_{wu}C_{u\tilde{u}} = \tilde{\mathbf{w}}C_{w\tilde{w}}^{-1}F_{wu}C_{u\tilde{u}}.$$

In particular, if a linear endomorphism $F : V \rightarrow V$ has the matrix $F_e \stackrel{\text{def}}{=} F_{ee}$ in some basis \mathbf{e} , then for another basis $\mathbf{u} = \mathbf{e}C_{eu}$, the matrix of F will be

$$F_u = C_{eu}^{-1} F_e C_{eu}. \quad (8.13)$$

8.4 Gaussian Elimination

Gaussian elimination simplifies a rectangular matrix while preserving its rank. This allows one to construct an explicit basis in a vector space given as the linear span of some vectors, or as the solution of systems of linear equations, or as a quotient space, etc. Gaussian elimination is the main computational tool in linear algebra. In some sense, it generalizes the Euclidean division algorithm.

8.4.1 Elimination by Row Operations

In this section we work in the coordinate space \mathbb{K}^n , whose vectors will be the rows. For every collection of such vectors

$$\begin{aligned} w_1 &= (w_{11}, w_{12}, \dots, w_{1n}), \\ w_2 &= (w_{21}, w_{22}, \dots, w_{2n}), \\ &\dots \\ w_k &= (w_{k1}, w_{k2}, \dots, w_{kn}), \end{aligned} \quad (8.14)$$

¹⁴See formula (6.20) on p. 136.

Gauss's method produces another collection of vectors u_1, u_2, \dots, u_r such that

$$\text{span}(u_1, u_2, \dots, u_r) = \text{span}(w_1, w_2, \dots, w_k),$$

and the coordinates of u_1, u_2, \dots, u_r written in rows,

$$\begin{pmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ u_{21} & u_{22} & \dots & u_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ u_{r1} & u_{r2} & \dots & u_{rn} \end{pmatrix},$$

form a *reduced echelon matrix*, meaning that the leftmost nonzero element of each row:

- is placed strictly to the right of the leftmost nonzero element of the previous row,
- is equal to 1,
- is the only nonzero element of its column.

A typical example of a reduced echelon matrix looks like this:

$$\begin{pmatrix} 0 & 1 & * & 0 & * & * & 0 & 0 & * \\ 0 & 0 & 0 & 1 & * & * & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * \end{pmatrix},$$

where asterisks indicate arbitrary constants. We write j_v for the number of the column containing the leftmost nonzero element of the v th row. The resulting strictly increasing sequence of numbers $J = (j_{v_1}, j_{v_2}, \dots, j_{v_r})$ is called the *shape* of the echelon matrix. The echelon matrix in the above example has shape $J = (2, 4, 7, 9)$.

Exercise 8.8 Verify that the nonzero rows of a reduced echelon matrix are linearly independent and thus form a basis of their linear span.

The reduction process splits into a sequence of elementary steps. In each step we take a collection of vectors v_1, v_2, \dots, v_ℓ and replace some pair of vectors v_i, v_j by their linear combinations $v'_i = av_i + bv_j$, $v'_j = cv_i + dv_j$ such that $\text{span}(v'_i, v'_j) = \text{span}(v_i, v_j)$. The latter property certainly holds for the following three *elementary row operations*:

- (1) $v'_i = v_i + \lambda v_j, \quad v'_j = v_j \quad (\text{with any } \lambda \in \mathbb{K}),$
- (2) $v'_i = v_j, \quad v'_j = v_i,$
- (3) $v'_i = \varrho v_i, \quad v'_j = v_j \quad (\text{with nonzero } \varrho \in \mathbb{K}),$

because the original v_i, v_j are linearly expressed through v'_i, v'_j as

$$\begin{aligned} (1)^{-1} \quad & v_i = v'_i - \lambda v'_j, & v_j &= v'_j, \\ (2)^{-1} \quad & v_i = v'_j, & v_j &= v'_i, \\ (3)^{-1} \quad & v_i = \varrho^{-1} v'_i, & v_j &= v'_j. \end{aligned}$$

The effect of these operations on the whole coordinate matrix (v_{ij}) of vectors v_i consists in

- (1) replacement of the i th row by its sum with the j th row multiplied by some $\lambda \in \mathbb{K}$,
 - (2) interchanging the i th and j th rows,
 - (3) multiplication of the i th row by some nonzero $\varrho \in \mathbb{K}$.
- (8.15)

Lemma 8.2 *Each matrix $A \in \text{Mat}_{m \times n}(\mathbb{K})$ can be transformed to some reduced echelon matrix by means of a finite sequence of elementary row operations.*

Proof We split the reduction procedure into n steps, where n is a number of columns. Assume inductively that after the $(k-1)$ th step, a submatrix formed by the left $k-1$ columns is in reduced echelon form¹⁵ and has s nonzero rows. Note that $0 \leq s \leq k-1$ and the $(m-s) \times (k-1)$ submatrix situated in the left-hand bottom corner is filled with zeros. At the k th step, we choose some nonzero element a situated in the k th column strictly below the s th row. If there is no such element, we can pass to the $(k+1)$ th step. If such an element a exists and is in the t th row, we multiply this row by a^{-1} . Then, if $t \neq s+1$, we interchange the $(s+1)$ th and t th rows. Thus, we get 1 at position $(s+1, k)$ and preserve the reduced echelon form of the submatrix formed by the leftmost $k-1$ columns. Finally, we annihilate all nonzero elements of the k th column except for the unit in the $(s+1)$ th row by adding appropriate multiples of the $(s+1)$ th row to all rows containing those nonzero elements. After that, we can proceed to the $(k+1)$ th step. \square

Example 8.8 (How It Works) Let us transform the matrix

$$A = \begin{pmatrix} 2 & -4 & -8 & 2 & -4 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix} \in \text{Mat}_{4 \times 5}(\mathbb{Q}) \quad (8.16)$$

¹⁵For $k=1$ this means nothing.

to reduced echelon form. Multiply the bottom row by -1 , and then swap it with the first row:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ 2 & -4 & -8 & 2 & -4 \end{pmatrix};$$

then eliminate the first column below the first row by adding to the second, third, and fourth rows the first row multiplied by 1, 1, and -2 respectively:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & -1 & -1 & 1 & -2 \\ 0 & -4 & -4 & 4 & -2 \end{pmatrix};$$

then eliminate the second column below the second row by adding the second row multiplied by 1 and by 4 to the third and fourth rows:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix};$$

then divide the third row by -2 and eliminate the last column outside the third row by adding appropriate multiples of the third row to the first and fourth rows:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (8.17)$$

We have obtained a reduced echelon matrix of shape $(1, 2, 5)$. The result shows that $\text{rk } A = 3$.

Example 8.9 (Basis in the Linear Span of Given Vectors) Since the elementary row operations do not change the linear span of the rows, the nonzero rows of the resulting reduced echelon matrix form a basis in the linear span of rows of the original matrix.¹⁶ For example, the computation from Example 8.8 shows that a

¹⁶See [Exercise 8.8](#) on p. 183.

subspace $U \subset \mathbb{Q}^5$ spanned by the rows of the matrix

$$\begin{pmatrix} 2 & -4 & -8 & 2 & -4 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix} \quad (8.18)$$

has dimension 3, and the rows of the matrix

$$\begin{pmatrix} 1 & 0 & -2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (8.19)$$

form a basis in U .

Proposition 8.1 *For every r -dimensional subspace $U \subset \mathbb{k}^n$, the standard basis of \mathbb{k}^n can be decomposed into two disjoint sets $\{e_{i_1}, e_{i_2}, \dots, e_{i_{n-r}}\} \sqcup \{e_{j_1}, e_{j_2}, \dots, e_{j_r}\} = \{e_1, e_2, \dots, e_n\}$ such that the complementary coordinate subspaces*

$$E_I = \text{span}(e_{i_1}, e_{i_2}, \dots, e_{i_{n-r}}) \simeq \mathbb{k}^{n-r} \quad \text{and} \quad E_J = \text{span}(e_{j_1}, e_{j_2}, \dots, e_{j_r}) \simeq \mathbb{k}^r$$

satisfy the following mutually equivalent conditions:

- (1) $U \cap E_I = 0$,
- (2) the quotient map $\pi : \mathbb{k}^n \twoheadrightarrow \mathbb{k}^n/U$ is restricted to the isomorphism $\pi|_{E_I} : E_I \xrightarrow{\sim} \mathbb{k}^n/U$,
- (3) the projection $p : \mathbb{k}^n \twoheadrightarrow E_J$, $(x_1, x_2, \dots, x_n) \mapsto (x_{j_1}, x_{j_2}, \dots, x_{j_r})$, of \mathbb{k}^n onto E_J along E_I is restricted to the isomorphism $p|_U : U \xrightarrow{\sim} E_J$,
- (4) there are r vectors $u_1, u_2, \dots, u_r \in U$ of the form $u_v = e_{j_v} + w_v$, where $w_v \in E_I$.

For every such decomposition $\mathbb{k}^n = E_I \oplus E_J$, the vectors u_v in (4) form a basis of U and are uniquely determined by U and the decomposition.

Proof For every basis w_1, w_2, \dots, w_r of U , the exchange lemma¹⁷ allows us to replace some r vectors $e_{j_1}, e_{j_2}, \dots, e_{j_r}$ of the standard basis in \mathbb{k}^n by vectors w_v in such a way that

$$w_1, w_2, \dots, w_r, e_{i_1}, e_{i_2}, \dots, e_{i_{n-r}}$$

is a basis in \mathbb{k}^n . This forces $E_I = \text{span}(e_{i_1}, e_{i_2}, \dots, e_{i_{n-r}})$ to satisfy condition (1). Now let us show that conditions (1)–(4) are equivalent. Condition (1) implies that $U \cap \ker p = E_I \cap \ker \pi = 0$. Hence both restricted maps $p|_U : U \rightarrow E_J$ and $\pi|_{E_I} : E_I \rightarrow \mathbb{k}^n/U$ are injective. Since the source and target spaces in both cases

¹⁷See Lemma 6.2 on p. 132.

have equal dimensions, both restricted maps are isomorphisms. Thus, (1) implies (2) and (3). Conversely, condition (2) (respectively (3)) implies the transversality of U (respectively of E_J) with $\ker \pi$ (respectively with $\ker p$). Such transversality is equivalent to (1). Condition (4) says that $p(u_v) = e_{j_v}$. If it holds, then p is an isomorphism. Conversely, if p is an isomorphism, there exists a unique basis $u_1, u_2, \dots, u_r \in U$ such that $p(u_v) = e_{j_v}$ for each v . \square

Remark 8.2 There are r -dimensional subspaces $U \subset \mathbb{k}^n$ transversal to all $(n - r)$ -dimensional coordinate subspaces E_I . Moreover, over an infinite ground field, a “typical” subspace is exactly of this sort. Thus for generic U , conditions (1)–(4) hold for many decompositions $\mathbb{k}^n = E_I \oplus E_J$, often for all. Gauss’s method indicates one of these decompositions, those with lexicographically minimal¹⁸ J , and explicitly computes the corresponding vectors u_1, u_2, \dots, u_r in (4). The latter feature is the main purpose of Gauss’s method.

Exercise 8.9 Let $A \in \text{Mat}_{k \times n}(\mathbb{k})$ be an arbitrary matrix, $U \subset \mathbb{k}^n$ the linear span of its rows, $J = (j_1, j_2, \dots, j_k)$ any shape satisfying $1 \leq j_1 < j_2 < \dots < j_k \leq n$. Show that U is isomorphically projected onto the coordinate subspace E_J along the complementary coordinate subspace E_I if and only if the $k \times r$ submatrix of A formed by the columns j_1, j_2, \dots, j_r has rank r .

Example 8.10 (Basis of a Quotient Space) Let R be a reduced echelon matrix of shape¹⁹ J . Write U for the linear span of its rows. Then the rows of R surely satisfy condition (4) of Proposition 8.1. Therefore, U is isomorphically projected onto the coordinate subspace E_J along the complementary coordinate subspace E_I , whereas the mod U congruence classes of the standard basic vectors $e_i \in E_I$ form a basis of the quotient space \mathbb{k}^n/U .

For example, one more consequence of the computation made in (8.19) is that the classes of vectors $e_3 = (0, 0, 1, 0, 0)$ and $e_4 = (0, 0, 0, 1, 0)$ form a basis in the quotient space \mathbb{Q}^5/U , where $U \subset \mathbb{Q}^5$ is the subspace spanned by the rows of the matrix

$$A = \begin{pmatrix} 2 & -4 & -8 & 2 & -4 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix}, \quad (8.20)$$

¹⁸See Sect. 8.4.2 on p. 190 below.

¹⁹Recall that the shape of an $r \times n$ echelon matrix is the increasing sequence of numbers $J = (j_{v_1}, j_{v_2}, \dots, j_{v_r})$ of the columns in which can be found the leftmost nonzero elements of the rows.

whose reduced echelon form is

$$R = \begin{pmatrix} 1 & 0 & -2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (8.21)$$

Example 8.11 (Solution of a Homogeneous System of Linear Equations) Associated with the matrix (8.20) is also the system of homogeneous linear equations

$$\begin{cases} 2x_1 - 4x_2 - 8x_3 + 2x_4 - 4x_5 = 0, \\ -x_1 + x_2 + 3x_3 + x_5 = 0, \\ -x_1 - x_2 + x_3 + 2x_4 - x_5 = 0, \\ -x_1 + 2x_3 + x_4 + x_5 = 0. \end{cases} \quad (8.22)$$

Its solution space is the annihilator $\text{Ann}(U) \subset \mathbb{Q}^{5*}$ of the linear subspace $\text{Ann } U \subset \mathbb{Q}^5$ spanned by the rows of the matrix A . If the linear form $\xi \in \mathbb{Q}^{5*}$ has coordinates (x_1, x_2, \dots, x_5) in the standard basis $e_1^*, e_2^*, \dots, e_5^*$ of \mathbb{Q}^{5*} dual to the standard basis e_1, e_2, \dots, e_5 in \mathbb{Q}^5 , then the value of ξ applied to the vector $a = (\alpha_1, \alpha_2, \dots, \alpha_5) \in \mathbb{Q}^5$ is $\xi(a) = a_1x_1 + a_2x_2 + \dots + a_5x_5$. Therefore, equations (8.22) say that ξ annihilates four vectors spanning U , that is, it annihilates U . Choosing another spanning system for U changes neither U nor $\text{Ann } U$. Thus, the system of equations with matrix (8.21),

$$\begin{cases} x_1 - 2x_3 - x_4 = 0, \\ x_2 + x_3 - x_4 = 0, \\ x_5 = 0, \end{cases} \quad (8.23)$$

is equivalent to the initial system (8.22). The system (8.23) has *separable unknowns*, that is, it can be rewritten in the form

$$\begin{cases} x_1 = 2x_3 + x_4, \\ x_2 = -x_3 + x_4, \\ x_5 = 0, \end{cases} \quad (8.24)$$

where the unknowns x_1, x_2, x_5 are expressed through the complementary unknowns x_3, x_4 . The left-hand-side unknowns, whose numbers form the shape of the reduced echelon matrix (8.21), are called *dependent*. The complementary unknowns are called *free*. They can take any values within $\mathbb{Q}^2 = E_{(3,4)}^*$, and for each $(x_3, x_4) \in \mathbb{Q}^2$, there exists a unique triple $(x_1, x_2, x_5) \in \mathbb{Q}^3 = E_{(1,2,5)}^*$ such that the total collection $(X_1, X_2, \dots, X_5) \in \mathbb{Q}^{5*}$ solves the system. Algebraically, x_1, x_2, x_5 are computed

from given x_3, x_4 by formulas (8.24). Geometrically, the projection along the coordinate space $E_{(1,2,5)}^* = \text{span}(e_1^*, e_2^*, e_5^*) \subset \mathbb{Q}^{5*}$ onto the complementary coordinate plane $E_{(3,4)}^* = \text{span}(e_3^*, e_4^*)$ gives an isomorphism $\text{Ann } U \simeq E_{(3,4)}^*$. Therefore, there exists a unique basis in $\text{Ann}(U)$ projected to the standard basis $e_3^*, e_4^* \in E_{(3,4)}^*$. It should consist of two forms looking like $\varphi_1 = (*, *, 1, 0, *)$, $\varphi_2 = (*, *, 0, 1, *)$. The coordinates marked by asterisks are easily determined from (8.24), which gives $\varphi_1 = (2, -1, 1, 0, 0)$, $\varphi_2 = (1, 1, 0, 1, 0)$. Thus, the solution space of the system (8.22) consists of all

$$(x_1, x_2, \dots, x_5) = \lambda_1 \varphi_1 + \lambda_2 \varphi_2 = (2\lambda_1 + \lambda_2, -\lambda_1 + \lambda_2, \lambda_1, \lambda_2, 0),$$

where (λ_1, λ_2) runs through \mathbb{Q}^2 . Every system with reduced echelon matrix of shape J can be solved in this way with the dependent unknowns numbered by J and the free unknowns numbered by the indices I complementary to J .

Example 8.12 (Solution of an Arbitrary System of Linear Equations) Given an arbitrary system of linear equations

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2, \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = b_3, \\ \qquad\qquad\qquad \dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m, \end{cases} \quad (8.25)$$

write $A = (a_{ij})$ for the $m \times n$ matrix of the coefficients on the left-hand side and $\tilde{A} = \begin{bmatrix} A & b \end{bmatrix}$ for the $m \times (n + 1)$ matrix constructed from A by attaching the right-hand-side column b to the right-hand side of A . The matrix \tilde{A} is called the *augmented matrix* of the system (8.25). In the language of equations, three elementary row operations (8.15) are applied to \tilde{A} :

- (1) add a multiple of the j th equation to the i th equation,
 - (2) swap the i th and j th equations,
 - (3) multiply both sides of the i th equation by an invertible constant.
- (8.26)

Exercise 8.10 Verify that these transformations take a system to an equivalent system, namely one that has the same solution set.

Thus, Gauss's method reduces a system of the form (8.25) to an equivalent system with reduced echelon augmented matrix $\tilde{R} = \begin{bmatrix} R & \beta \end{bmatrix} \in \text{Mat}_{r \times (n+1)}(\mathbb{K})$, where $r = \text{rk } \tilde{R} = \text{rk } \tilde{A}$, $R = (\alpha_{ij}) \in \text{Mat}_{r \times r}(\mathbb{K})$. Such a reduced echelon system has separable unknowns and can be solved exactly in the same way as in the previous example. Namely, let $J = (j_{v_1}, j_{v_2}, \dots, j_{v_r})$ be the shape of \tilde{R} . If $j_r = n + 1$, then the r th

equation is $0 = 1$, and the system is inconsistent. Note that in this case,

$$\operatorname{rk} A = \operatorname{rk} R = r - 1 \neq r = \operatorname{rk} \tilde{R} = \operatorname{rk} \tilde{A},$$

and this agrees with the Capelli–Fontené–Frobenius–Kronecker–Rouché theorem, Theorem 7.4 on p. 166.

If $j_r \leq n$, then $\operatorname{rk} R = \operatorname{rk} \tilde{R} = r$, and the dependent unknowns x_j with $j \in J$ are expressed through the complementary unknowns $x_i \in I = \{1, 2, \dots, n\} \setminus J$ as

$$\begin{aligned} x_{j_1} &= \beta_1 - \alpha_{1i_1}x_{i_1} - \alpha_{1i_2}x_{i_2} - \cdots - \alpha_{1i_{n-r}}x_{i_{n-m}}, \\ x_{j_2} &= \beta_2 - \alpha_{2i_1}x_{i_1} - \alpha_{2i_2}x_{i_2} - \cdots - \alpha_{2i_{n-r}}x_{i_{n-m}}, \\ &\dots \\ x_{j_r} &= \beta_r - \alpha_{ri_1}x_{i_1} - \alpha_{ri_2}x_{i_2} - \cdots - \alpha_{ri_{n-r}}x_{i_{n-m}}. \end{aligned} \tag{8.27}$$

This gives a parametric representation of all solutions: take any $(x_{i_1}, x_{i_2}, \dots, x_{i_{n-r}}) \in \mathbb{k}^{n-r} = E_I$ and compute the remaining x_j by the formulas (8.27). For example, taking all free unknowns to be zero, we get the solution $x_{i_v} = \beta_v, x_{j_\mu} = 0$.

Example 8.13 (Graphs of Linear Maps) Let a linear subspace $U \subset \mathbb{k}^n$ and the decomposition $\mathbb{k}^n = E_I \oplus E_J$ satisfy the conditions of Proposition 8.1. Then U can be viewed as the graph of the linear map $f_U = p_I \circ p_J^{-1} : E_J \rightarrow E_I$, where $p_I : U \rightarrow E_I$ and $p_J : U \xrightarrow{\sim} E_J$ are the projections. For every $v \in E_J$, the vector $f_U(v) \in E_I$ is uniquely determined by the prescription $v + f_U(v) \in U$, because the projection $p_J : U \xrightarrow{\sim} E_J$ is bijective. Let the rows u_1, u_2, \dots, u_r of the reduced echelon matrix R form a basis of U . Then $p_J^{-1}(e_{j_v}) = u_v$, and therefore $f_U(e_{j_v})$ is the v th row of the submatrix $R_I \subset R$ formed by the columns $i_{v_1}, i_{v_2}, \dots, i_{v_{n-r}}$. In other words, the matrix of the linear map f_U in the standard bases is R_I^t , the transposed submatrix $R_I \subset R$ formed by rows indexed by I .

8.4.2 Location of a Subspace with Respect to a Basis

In this section we show that the reduced echelon matrix A_{red} obtained from a given matrix A by means of Gaussian elimination is predicted by the subspace $U \subset \mathbb{k}^n$ spanned by the rows of A and does not depend on the particular sequence of elementary row operations used in the reduction procedure. Let us write $V^i = \operatorname{span}(e_{i+1}, e_{i+2}, \dots, e_n)$ for the linear span of the last $n - i$ standard basis vectors in \mathbb{k}^n . The coordinate subspaces V^i form a decreasing chain

$$\mathbb{k}^n = V^0 \supset V^1 \supset V^2 \supset \cdots \supset V^{n-1} \supset V^n = 0, \tag{8.28}$$

called a *complete coordinate flag*. Let $\pi_i : V^0 \twoheadrightarrow V^0/V^i$ denote the quotient map. Roughly speaking, $\pi_i(v)$ is “ v considered up to the last $(n-i)$ coordinates.” Associated with every r -dimensional vector subspace $U \subset V$ is a collection of nonnegative integers

$$d_i \stackrel{\text{def}}{=} \dim \pi_i(U) = r - \dim \ker \pi_i|_U = r - \dim U \cap V^i, \quad 0 \leq i \leq n.$$

The numbers d_0, d_1, \dots, d_n form a nondecreasing sequence beginning with $d_0 = 0$ and ending with $d_n = r$. All the increments $d_i - d_{i-1}$ are less than or equal to 1, because $U \cap V^i$ is contained in the linear span of $U \cap V^{i+1}$ and e_i , the dimension of which is at most 1 greater than $\dim(U \cap V^{i+1})$. Write $J = (j_1, j_2, \dots, j_r)$ for the collection of the r indices for which $d_{j_v} - d_{j_v-1} = 1$ and call it the *combinatorial type* of the subspace U with respect to the coordinate flag (8.28). For example, the subspace $U \subset \mathbb{Q}^5$ spanned by the rows of echelon matrix

$$\begin{pmatrix} 1 & 0 & 2 & 3 & 0 \\ 0 & 1 & 4 & 5 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (8.29)$$

has dimensions $(d_0, d_1, \dots, d_5) = (0, 1, 2, 2, 2, 3)$ and has combinatorial type $J = (1, 2, 5)$.

Exercise 8.11 Let $U \subset \mathbb{K}^n$ be spanned by the rows of the reduced echelon matrix $R \in \text{Mat}_{r \times n}(\mathbb{K})$. Show that the combinatorial type of U coincides with the shape of R .

Therefore, the shape of A_{red} depends only on the linear span U of the rows of A . A subspace U of combinatorial type J satisfies Proposition 8.1 on p. 186 for the decomposition $\mathbb{K}^n = E_I \oplus E_J$, where $I = \{1, 2, \dots, n\} \setminus J$. Hence, by Proposition 8.1, the rows of A_{red} , which form the basis $u_1, u_2, \dots, u_r \in U$ projected along E_I to the standard basis $e_{j_1}, e_{j_2}, \dots, e_{j_r}$ in E_J , are uniquely determined by U and the decomposition $\mathbb{K}^n = E_I \oplus E_J$. We conclude that the reduced echelon matrix A_{red} depends only on $U \subset \mathbb{K}^n$. We summarize the discussion as follows.

Proposition 8.2 *Every subspace $U \subset \mathbb{K}^n$ admits a unique basis u_1, u_2, \dots, u_r such that the coordinates of the basis vectors written in rows form a reduced echelon matrix M_U . The assignment $U \mapsto M_U$ establishes a bijection between the r -dimensional subspaces $U \subset \mathbb{K}^n$ and the reduced echelon matrices of width n with exactly r nonzero rows.* \square

Exercise 8.12 Show that the reduced echelon matrices of shape (j_1, j_2, \dots, j_r) form an affine subspace of dimension $r(n-r) - \sum_{v=1}^r (j_v - v + 1)$ in $\text{Mat}_{r \times n}(\mathbb{K})$.

8.4.3 Gaussian Method for Inverting Matrices

We know from the examples appearing after formula (8.3) on p. 177 that each elementary row operation (8.15) on $m \times n$ matrices is realized as left multiplication by an appropriate $m \times m$ matrix L , which depends only on the operation but not on the matrix to which the operation is applied. In other words, each row operation is a map of type

$$\text{Mat}_{m \times n}(\mathbb{k}) \rightarrow \text{Mat}_{m \times n}(\mathbb{k}), \quad A \mapsto LA.$$

Exercise 8.13 Verify that the matrix L realizing a row operation is equal to the result of this operation applied to the $m \times m$ identity matrix E .

As we have seen before (8.15), for every elementary row operation, there is an inverse row operation that recovers the original matrix from the transformed one. Write L' for the $m \times m$ matrix multiplication by that realizes the row operation inverse to that provided by the left multiplication by a matrix L . Thus, $L'LA = A$ for every $A \in \text{Mat}_{m \times n}(\mathbb{k})$. Similarly, there exists a matrix L'' such that $L''L'A = A$ for all A . Taking $A = E$, we get $L''L' = L''L'E = E = L'LE = L'/L$. Hence, $L'' = L = (L')^{-1}$. We conclude that each elementary row operation is realized as left multiplication by an *invertible* $m \times m$ matrix.

Exercise 8.14 Verify that the product of invertible matrices is invertible and

$$(L_1 \cdot L_2 \cdots L_k)^{-1} = L_k^{-1} L_{k-1}^{-1} \cdots L_1^{-1}.$$

Let A be a square $n \times n$ matrix. As we have just seen, every matrix B obtained from A by elementary row operations can be written as $B = LA$ for an invertible matrix L constructed from the identity matrix E by the same sequence of row operations that creates B from A . If B has a reduced echelon form, then either $B = E$ or the bottom row in B vanishes. In the second case, $\text{rk } B = \text{rk } A < n$, and therefore both matrices B, A are noninvertible, because the linear endomorphisms $\mathbb{k}^n \rightarrow \mathbb{k}^n$ given by these matrices in the standard basis of \mathbb{k}^n are not surjective. In the first case, $LA = E$ for some invertible matrix L . Therefore $A = L^{-1}$ is invertible and $A^{-1} = L$ is constructed from E by the same sequence of elementary row operations that constructs E from A .

In other words, to check whether a given matrix $A \in \text{Mat}_n(\mathbb{k})$ is invertible, we can proceed as follows. Form the $n \times 2n$ matrix $\begin{bmatrix} A & E \end{bmatrix}$ by attaching the identity matrix E to the right of A . Use Gaussian elimination to transform $\begin{bmatrix} A & E \end{bmatrix}$ to the reduced echelon matrix $\begin{bmatrix} B & C \end{bmatrix}$. If during this transformation, the left $n \times n$ half matrix

becomes noninvertible,²⁰ then A is not invertible. If the resulting echelon matrix has $B = E$, then $C = A^{-1}$.

Example 8.14 Let us analyze whether the matrix

$$A = \begin{pmatrix} 6 & 3 & -2 & 1 \\ 1 & 4 & 1 & 1 \\ 1 & 1 & 3 & -1 \\ -1 & 0 & -2 & 1 \end{pmatrix}$$

is invertible, and if it is, compute the inverse by Gaussian row elimination in the extended matrix

$$\left(\begin{array}{cccc|cccc} 6 & 3 & -2 & 1 & 1 & 0 & 0 & 0 \\ 1 & 4 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 3 & -1 & 0 & 0 & 1 & 0 \\ -1 & 0 & -2 & 1 & 0 & 0 & 0 & 1 \end{array} \right).$$

Change the sign of the bottom row and swap the top row with the bottom:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 1 & 4 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 3 & -1 & 0 & 0 & 1 & 0 \\ 6 & 3 & -2 & 1 & 1 & 0 & 0 & 0 \end{array} \right).$$

Annihilate the first column below the first row by adding appropriate multiples of the first row to all other rows:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 4 & -1 & 2 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 3 & -14 & 7 & 1 & 0 & 0 & 6 \end{array} \right).$$

Swap the two middle rows and annihilate the second column below the second row:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & -5 & 2 & 0 & 1 & -4 & -3 \\ 0 & 0 & -17 & 7 & 1 & 0 & -3 & 3 \end{array} \right). \quad (8.30)$$

²⁰For example, if one row becomes proportional to another.

Now, to avoid fractions, let us digress from the classical procedure and transform the two bottom rows by means of the invertible matrix²¹

$$\begin{pmatrix} -5 & 2 \\ -17 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} -7 & 2 \\ -17 & 5 \end{pmatrix},$$

that is, multiply the whole 4×4 matrix from the left by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -7 & 2 \\ 0 & 0 & -17 & 5 \end{pmatrix}.$$

Exercise 8.15 Verify that this matrix is invertible.

We get

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 2 & -7 & 22 & 27 \\ 0 & 0 & 0 & 1 & 5 & -17 & 53 & 66 \end{array} \right).$$

Finally, subtract the third row from the second and fourth rows and twice the third row from the first:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & -3 & 9 & 11 \\ 0 & 1 & 0 & 0 & -2 & 7 & -21 & -26 \\ 0 & 0 & 1 & 0 & 2 & -7 & 22 & 27 \\ 0 & 0 & 0 & 1 & 5 & -17 & 53 & 66 \end{array} \right).$$

We conclude that the matrix A is invertible and

$$A^{-1} = \begin{pmatrix} 1 & -3 & 9 & 11 \\ -2 & 7 & -21 & -26 \\ 2 & -7 & 22 & 27 \\ 5 & -17 & 53 & 66 \end{pmatrix}.$$

²¹See formula (8.7) on p. 179.

are defined by the same rules,

$$s_{ij} = f_{ij} + g_{ij} \quad \text{and} \quad p_{ij} = \sum_v f_{iv} g_{vj},$$

as for matrices over commutative rings.

Exercise 8.17 Check associativity and both distributivity properties of these operations.

The ring of square $n \times n$ matrices with elements in a ring R is denoted by $\text{Mat}_n(R)$ and called the *order- n matrix algebra* over R . One should be careful when making computations with matrices whose elements do not commute and are not invertible. For example, formula (8.5) on p. 179 becomes incorrect over a noncommutative ring R , because we permuted matrix element factors in the products when we took the common factor $(a + d)$ out of the secondary diagonal of the matrix. Formula (8.7) for the inverse matrix also fails over a noncommutative ring. Even over a commutative ring that is not a field, the invertibility criterion should be formulated more accurately: a 2×2 matrix F over a commutative ring is invertible if and only if $\det F$ is invertible, and in this case, formula (8.7) for the inverse matrix holds.

Exercise 8.18 Prove the latter statement.

Example 8.16 (Some Invertible 2×2 Matrices) Over an arbitrary ring R , an upper triangular matrix

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

is invertible if and only if both diagonal elements a, d are invertible in R . Indeed, the equality

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bw \\ dz & dw \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

leads to $dw = 1$ and $dz = 0$. Thus, d is invertible, $w = d^{-1}$, and $z = 0$. This gives $ax = 1$ and $ay + bd^{-1} = 0$ in the upper row. Hence, $x = a^{-1}$, $y = -a^{-1}bd^{-1}$, and

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}bd^{-1} \\ 0 & d^{-1} \end{pmatrix}.$$

Similar arguments show that a lower triangular matrix

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$$

is invertible if and only if a, d are both invertible, and in this case,

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & 0 \\ -d^{-1}ca^{-1} & d^{-1} \end{pmatrix}.$$

Exercise 8.19 Show that matrices $\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$ are invertible if and only if c, b are both invertible, and in this case,

$$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & c^{-1} \\ b^{-1} & -b^{-1}ac^{-1} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} -c^{-1}db^{-1} & c^{-1} \\ b^{-1} & 0 \end{pmatrix}.$$

The above calculations show that Gaussian elementary row operations of the first type, which replace a row by its sum with any multiple of another row, are realized by left multiplication by *invertible* matrices even over noncommutative rings.

Example 8.17 (Unitriangular Matrices) The two diagonals beginning at the upper left and right corners of a square matrix

$$\begin{pmatrix} * & & \\ & * & \\ & & * \end{pmatrix}, \quad \begin{pmatrix} & * & \\ & & * \\ * & & \end{pmatrix}$$

are called the *main* and *secondary* diagonals respectively. A square matrix $A = (a_{ij})$ is called *upper* (respectively *lower*) *triangular* if all matrix elements below (respectively above) the main diagonal vanish, i.e., if $a_{ij} = 0$ for all $i > j$ (respectively for all $i < j$). Over a ring with unit, a triangular matrix is called *unitriangular* if all the diagonal elements equal 1.

Exercise 8.20 Check that upper and lower triangular and unitriangular matrices form subrings in $\text{Mat}_n(R)$.

We are going to show that every upper unitriangular matrix $A = (a_{ij})$ over an arbitrary ring with unit is invertible and that the elements b_{ij} of the inverse matrix $B = A^{-1}$ are given by the formula

$$\begin{aligned} b_{ij} &= \sum_{s=0}^{j-i-1} (-1)^{s+1} \sum_{i < v_1 < \dots < v_s < j} a_{iv_1} a_{v_1 v_2} a_{v_2 v_3} \cdots a_{v_{s-1} v_s} a_{v_s j} \\ &= -a_{ij} + \sum_{i < k < j} a_{ik} a_{kj} - \sum_{i < k < \ell < j} a_{ik} a_{k\ell} a_{\ell j} + \sum_{i < k < \ell < m < j} a_{ik} a_{k\ell} a_{\ell m} a_{mj} - \cdots. \end{aligned} \tag{8.31}$$

We proceed by Gaussian elimination. For a 4×4 matrix

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} \\ 0 & 1 & a_{23} & a_{24} \\ 0 & 0 & 1 & a_{34} \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

the computation is as follows. Attach the identity matrix from the right:

$$\left(\begin{array}{cccc|cccc} 1 & a_{12} & a_{13} & a_{14} & 1 & 0 & 0 & 0 \\ 0 & 1 & a_{23} & a_{24} & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & a_{34} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array} \right).$$

Annihilate the second column over the main diagonal by adding the appropriate multiple of the second row to the first:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & a_{13} - a_{12}a_{23} & a_{14} - a_{12}a_{24} & 1 & -a_{12} & 0 & 0 \\ 0 & 1 & a_{23} & a_{24} & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & a_{34} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array} \right).$$

Annihilate the third column over the main diagonal by adding appropriate multiples of the third row to the first and the second rows:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & a_{14} - a_{12}a_{24} - a_{13}a_{34} + a_{12}a_{23}a_{34} & 1 & -a_{12} & -a_{13} + a_{12}a_{23} & 0 \\ 0 & 1 & 0 & a_{24} - a_{23}a_{34} & 0 & 1 & -a_{23} & 0 \\ 0 & 0 & 1 & a_{34} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array} \right).$$

Finally, annihilate the last column over the main diagonal by adding appropriate multiples of the last row to all the other rows:

$$A^{-1} = \begin{pmatrix} 1 & -a_{12} & -a_{13} + a_{12}a_{23} & -a_{14} + a_{12}a_{24} + a_{13}a_{34} - a_{12}a_{23}a_{34} \\ 0 & 1 & -a_{23} & -a_{24} + a_{23}a_{34} \\ 0 & 0 & 1 & -a_{23} \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

To explain the general case, let us mark n distinct points $1, 2, \dots, n$ on a plane and depict a matrix element a_{ij} by an arrow drawn from j to i . We think of right multiplication by a_{ij} as a passage from i to j along this arrow. Then every directed

passage formed by s sequential arrows

$$\overrightarrow{k_0 k_1}, \overrightarrow{k_1 k_2}, \overrightarrow{k_3 k_4}, \dots, \overrightarrow{k_{s-2} k_{s-1}}, \overrightarrow{k_{s-1} k_s}, \text{ where } k_0 < k_1 < \dots < k_s,$$

corresponds to the product $a_{k_0 k_1} a_{k_1 k_2} a_{k_2 k_3} \cdots a_{k_{s-2} k_{s-1}} a_{k_{s-1} k_s}$ of s matrix elements in R . Under this visualization, formula (8.31) says that the element b_{ij} is equal to the sum of all oriented passages going from i to j , where all s -step passages are taken with sign $(-1)^s$.

Now consider the $n \times (2n)$ matrix $\begin{bmatrix} A & E \end{bmatrix}$ and multiply it from the left by the matrix

$$S = \begin{pmatrix} 1 & b_{12} & b_{13} & \cdots & b_{1(n-1)} & 0 \\ 0 & 1 & b_{23} & \cdots & b_{2(n-1)} & 0 \\ & & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & b_{(n-2)(n-1)} & 0 \\ 0 & \cdots & \cdots & 0 & 1 & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix},$$

whose left upper $(n-1) \times (n-1)$ submatrix is inverse to the left upper $(n-1) \times (n-1)$ submatrix of A by induction. Let $C \stackrel{\text{def}}{=} SA$ and write $S \begin{bmatrix} A & E \end{bmatrix} = \begin{bmatrix} C & S \end{bmatrix}$ for the product. Then the left upper $(n-1) \times (n-1)$ submatrix of C equals the identity matrix, the bottom rows of $\begin{bmatrix} A & E \end{bmatrix}$ and $\begin{bmatrix} C & S \end{bmatrix}$ coincide, and the n th column of C consists of elements

$$c_{in} = a_{in} + b_{i2}a_{2n} + b_{i3}a_{3n} + \cdots + b_{i(n-1)}a_{(n-1)n}.$$

By induction, the latter sum is formed by all oriented passages from n to i , where all $(s+1)$ -step passages are taken with the sign $(-1)^s$. Eliminating the n th column of C over the main diagonal by adding appropriate multiples of the bottom row to all the other rows, we get in the rightmost column of the resulting $n \times (2n)$ matrix exactly those values b_{in} predicted by (8.31).

Problems for Independent Solution to Chap. 8

Problem 8.1 For a ring R , the subring $Z(R) \stackrel{\text{def}}{=} \{c \in R \mid \forall x \in R \, cx = xc\}$ is called the *center* of R . Describe $Z(\text{Mat}_n(K))$, where K is an arbitrary commutative ring with unit.

Problem 8.2 For every square matrix of rank 1 over a field \mathbb{k} , show that $A^2 = \lambda A$ for some $\lambda \in \mathbb{k}$.

Problem 8.3 Realize the following transformations of a rectangular matrix over a commutative ring K via multiplication by an appropriate matrix B from the

appropriate side²⁴: **(a)** swap the i th and j th rows, **(b)** multiply row i by $\lambda \in K$, **(c)** replace the i th row by its sum with the j th row multiplied by $\lambda \in K$, **(d)** similar transformations of columns.

Problem 8.4 For the matrices

$$\begin{pmatrix} -2 & -1 & -7 & 5 & -4 \\ -1 & 4 & 1 & -2 & 1 \\ -1 & -2 & -5 & 4 & -3 \\ 1 & -1 & 2 & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & -1 & 0 & -1 & 0 \\ -2 & -2 & 1 & 2 & 0 \\ -7 & -1 & 2 & 2 & -2 \\ 4 & 0 & -1 & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 3 & -6 & 2 & -5 \\ 7 & -2 & 3 & -2 & 0 \\ -1 & 0 & -2 & 1 & -2 \\ -4 & 0 & -1 & 1 & 0 \end{pmatrix},$$

explicitly choose a basis in the **(a)** linear span of the columns, **(b)** linear span of the rows, **(c)** annihilator of the linear span of the rows, **(d)** quotient of \mathbb{Q}^5 by the linear span of rows, **(e)** quotient of \mathbb{Q}^4 by the annihilator of the linear span of the columns **(f)** dual vector space to the quotient of \mathbb{Q}^5 by the linear span of the rows.

Problem 8.5 Explicitly indicate some basis in the sums and intersections of the following pairs of vector subspaces in \mathbb{Q}^4 :

- (a)** linear spans of vectors $(1, 1, 1, 1)$, $(1, -1, 1, -1)$, $(1, 3, 1, 3)$ and $(1, 2, 0, 2)$, $(1, 2, 1, 2)$, $(3, 1, 3, 1)$,
- (b)** linear span of vectors $(1, 1, 0, 0)$, $(0, 1, 1, 0)$, $(0, 0, 1, 1)$ and solution space of equations $x_1 + x_3 = 2x_2 + x_3 + x_4 = x_1 + 2x_2 + x_3 + 2x_4 = 0$,
- (c)** solution space of equations $x_1 + x_2 = x_2 + x_3 = x_3 + x_4 = 0$, and solution space of equations $x_1 + 2x_2 + 2x_4 = x_1 + 2x_2 + x_3 + 2x_4 = 3x_1 + x_2 + 3x_3 + x_4 = 0$.

Problem 8.6 For the following pairs of vector subspaces in \mathbb{Q}^4 , find:

- (a)** the linear span of the vectors $(-11, 8, -1, 2)$, $(-6, 5, 2, 3)$, $(-3, 2, -1, 0)$ and the linear span of vectors $(-8, 4, 12, -4)$, $(-6, -5, -9, 1)$, $(-2, -3, -6, 1)$,
- (b)** the linear span of the vectors $(30, 5, -9, 1)$, $(2, 8, 4, -3)$, $(-6, -4, 0, 1)$ and solution space of the linear equations

$$2x_1 + 3x_2 - 4x_3 + x_4 = -x_1 - 2x_2 + 3x_3 - x_4 = -x_2 + 2x_3 - x_4 = 0.$$

- (c)** the solution spaces of the linear equations

$$\begin{cases} -3x_1 - 10x_2 + 20x_3 - 6x_4 = 0, \\ -15x_1 + 4x_2 + 19x_3 - 3x_4 = 0, \\ 6x_1 - 10x_3 + 2x_4 = 0, \end{cases} \quad \text{and} \quad \begin{cases} 6x_1 - 7x_2 - 3x_3 - 2x_4 = 0, \\ -7x_1 - x_2 + 6x_3 - x_4 = 0, \\ 5x_1 - 4x_2 - 3x_3 - x_4 = 0. \end{cases}$$

²⁴Give the side and explicitly write B .

Select the complementary pairs of subspaces, and for each such pair, project the standard basis vectors of \mathbb{Q}^4 to the first subspace along the second.

Problem 8.7 Verify that the annihilator of the linear form $x_1 + x_2 + \cdots + x_n$ and the solution space of $(n-1)$ linear equations $x_1 = x_2 = \cdots = x_n$ are complementary in \mathbb{Q}^n . Project the standard basis vectors of \mathbb{Q}^n to the first subspace along the second.

Problem 8.8 Drawn on a sheet of graph paper is an $m \times n$ rectangle formed by segments of the grid lines joining four points where two lines intersect. The cells of an external circuit of the rectangle are filled by some rational numbers. Prove that the internal cells of the rectangle can be filled with rational numbers in such a way that each element equals the arithmetic mean of its eastern, northern, western, and southern neighbors. How many such fillings are possible?

Problem 8.9 Six edges of a regular tetrahedron are marked by rational numbers b_1, b_2, \dots, b_6 . Let us call such a marking admissible if there exists a marking of four faces of the tetrahedron by rational numbers such that the sum of the numbers on each pair of faces equals the number on their common edge. Find all admissible markings $(b_1, b_2, \dots, b_6) \in \mathbb{Q}^6$, and for each of them describe all compatible markings of faces.

Problem 8.10 Eight vertices of a cube are marked by rational numbers b_1, b_2, \dots, b_8 . Call such a marking admissible if there exists a marking of six faces of the cube by rational numbers such that the number on each vertex equals the sum of numbers on three faces sharing this vertex. Find all admissible markings $(b_1, b_2, \dots, b_8) \in \mathbb{Q}^8$, and for each of them, describe all compatible markings of faces.

Problem 8.11 For nonzero $a \in \mathbb{C}$, find $\begin{pmatrix} a & 1 & 1 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}^{-1}$.

Problem 8.12 For arbitrarily given $a_1, a_2, \dots, a_n \in \mathbb{N}$, consider the matrix $A \in \text{Mat}_n(\mathbb{C})$ with elements $e^{2\pi i/a_k}$ on the secondary diagonal and zeros in all other places. Find the minimal $m \in \mathbb{N}$ such that $A^m = E$.

Problem 8.13 (Commutators) Given two square matrices $A, B \in \text{Mat}_n(\mathbb{k})$ over a field \mathbb{k} , the difference $[A, B] \stackrel{\text{def}}{=} AB - BA$ is called the *commutator* of A, B . For all $A, B, C \in \text{Mat}_n(\mathbb{k})$, prove the *Leibniz rules*: (a) $[A, BC] = [A, B]C + B[A, C]$, (b) $[A, [B, C]] = [[A, B], C] + [B, [A, C]]$.

Problem 8.14 Express $(A + B)^n$ through $A^i B^j$ if (a) $[A, B] = 0$, (b*) $[A, B] = B$, (c*) $[A, B] = A$.

Problem 8.15 (Trace) The sum of all the elements on the main diagonal of a square matrix A is called the *trace* of A and is denoted by $\text{tr } A \stackrel{\text{def}}{=} \sum_i a_{ii}$. In the matrix algebra $\text{Mat}_n(K)$ over a commutative ring K , prove that (a) $\text{tr}[A, B] = 0$ for all A, B , (b) $\text{tr}(C^{-1}AC) = \text{tr}(A)$ for every A and invertible C .

Problem 8.16 In the vector space $\text{Mat}_n(\mathbb{k})$ over a field \mathbb{k} , consider a system of linear equations $\text{tr}(AX) = 0$ in the unknown matrix X , where $A \in \text{Mat}_n(\mathbb{k})$ runs through

all matrices with nonzero trace. Show that the solution space of this system is the 1-dimensional space of scalar matrices $X = \lambda E$, $\lambda \in \mathbb{k}$.

Problem 8.17 (Nilpotent Matrices) A square matrix A is called *nilpotent* if $A^n = 0$ for some $n \in \mathbb{N}$. Assuming that $A, B \in \text{Mat}_n(\mathbb{k})$ are nilpotent, show that: **(a)** $A + B$ is not necessarily nilpotent, **(b)** if $[A, B] = 0$, then $A + B$ is nilpotent, **(c*)** if $[A, [A, B]] = [B, [B, A]] = 0$, then $A + B$ is nilpotent.

Problem 8.18 (Unipotent Matrices) A square matrix A over a field \mathbb{k} is called *unipotent* if $E - A$ is a nilpotent matrix. Show that

- (a)** if $\text{char } \mathbb{k} = p > 0$, then $A \in \text{Mat}_n(\mathbb{k})$ is unipotent if and only if $A^m = E$ for some $m \in \mathbb{N}$,
(b) if $\text{char } \mathbb{k} = 0$, then $A \in \text{Mat}_n(\mathbb{k})$ is unipotent if and only if

$$A = e^N = \sum_{k \geq 0} N^k / k! = E + N + \frac{1}{2}N^2 + \frac{1}{6}N^3 + \dots$$

for some nilpotent matrix $N \in \text{Mat}_n(\mathbb{k})$ (note that for all such N , the sum is finite).

Problem 8.19 Solve the following equations in the unknown matrix $X \in \text{Mat}_2(\mathbb{C})$:
(a) $X^2 = 0$, **(b)** $X^3 = 0$, **(c)** $X^2 = X$, **(d)** $X^2 = E$, **(e)** $X^2 = -E$.

Problem 8.20 For matrices A, B, C of sizes $k \times \ell$, $\ell \times m$, $m \times n$, prove that
(a) $\text{rk}(AB) \leq \min(\text{rk } A, \text{rk } B)$, **(b)** $\text{rk}(AB) + \text{rk}(BC) \leq \text{rk}(ABC) + \text{rk}(B)$,
(c) $\text{rk}(A) + \text{rk}(B) \leq \text{rk}(AB) + \ell$.

Problem 8.21 Let $W = V \oplus V$, where $V = \mathbb{k}^n$, \mathbb{k} a field.

- (a)** Show that $\text{End}(W) \simeq \text{Mat}_{2 \times 2}(\text{End}(V))$.
(b) For an invertible matrix $A \in \text{Mat}_n(\mathbb{k})$ and arbitrary matrices $B, C, D \in \text{Mat}_n(\mathbb{k})$ such that $\text{rk} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = n$, show that $D = CA^{-1}B$.
(c) For invertible matrices $A, B, C, D \in \text{Mat}_n(\mathbb{k})$, show that the matrices $A - BD^{-1}C$, $C - DB^{-1}A$, $B - AC^{-1}D$, $D - CA^{-1}B$ are invertible in $\text{Mat}_n(\mathbb{k})$. Check that in $\text{Mat}_{2n}(\mathbb{k})$,

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} = \begin{pmatrix} (A - BD^{-1}C)^{-1} & (C - DB^{-1}A)^{-1} \\ (B - AC^{-1}D)^{-1} & (D - CA^{-1}B)^{-1} \end{pmatrix}.$$

Problem 8.22 (Möbius Inversion Formula) A poset²⁵ P is called *locally finite* if it has a lower bound²⁶ $p_* \in P$ and for all $x, y \in P$, the *segment*

$$[x, y] \stackrel{\text{def}}{=} \{z \in P \mid x \leq z \leq y\}$$

²⁵See Sect. 1.4 on p. 13.

²⁶That is, if there is $p_* \in P$ such that $m \leq x$ for all $x \in P$.

is finite. For a locally finite poset P , write $\mathcal{A} = \mathcal{A}(P)$ for the set of all functions $\varrho : P \times P \rightarrow \mathbb{R}$ such that $\varrho(x, y) \neq 0$ only if $x \leq y$. Define addition and a multiplication in \mathcal{A} by

$$\begin{aligned}\varrho_1 + \varrho_2 &: (x, y) \mapsto \varrho_1(x, y) + \varrho_2(x, y), \\ \varrho_1 * \varrho_2 &: (x, y) \mapsto \sum_{x \leq z \leq y} \varrho_1(x, z) \varrho_2(z, y).\end{aligned}$$

- (a) Show that \mathcal{A} is an associative \mathbb{R} -algebra with unit and $\varrho \in \mathcal{A}$ is invertible if and only if $\varrho(x, x) \neq 0$ for all $x \in P$.
 (b) Define the *Möbius function* $\mu \in \mathcal{A}$ to be the element inverse to the *zeta function*

$$\zeta(x, y) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } x \leq y, \\ 0 & \text{otherwise.} \end{cases}$$

Show that $\mu(x, y) = -\sum_{x \leq z < y} \mu(x, z) = -\sum_{x < z \leq y} \mu(z, y)$.

- (c) For a function $g : P \rightarrow \mathbb{R}$, the function $\sigma_g(x) \stackrel{\text{def}}{=} \sum_{y < x} g(y)$ is called the *Möbius transform* of g . Show that g is uniquely recovered from σ_g by the following *Möbius inversion formula*:

$$g(x) = \sum_{y < x} \sigma(y) \mu(y, x).$$

- (d) Give a precise intrinsic description of the Möbius inversion formula for $P = \mathbb{N}$ partially ordered by the divisibility relation $n \mid m$ (compare with [Problem 2.20](#) on p. 39).
 (e) For a set X , give a precise intrinsic description of the Möbius inversion formula in the set of all finite subsets of X partially ordered by inclusion and compare the answer with the combinatorial inclusion–exclusion principle.
 (f) Deduce the inversion formula for upper unitriangular matrices in [Example 8.17](#) on p. 197 from the Möbius inversion formula.

Problem 8.23 For a linear endomorphism $F : V \rightarrow V$ of a finite-dimensional vector space V over a field \mathbb{k} , show that the minimal polynomial²⁷ $\mu_F(x)$ of F is divisible in $\mathbb{k}[x]$ by the products $\prod (x - \lambda)$ taken over any sets of mutually distinct eigenvalues²⁸ $\lambda \in \mathbb{k}$ of F .

Problem 8.24 Find the kernel, the images, and the minimal polynomial for both difference operators $\Delta : f(x) \mapsto f(x + 1) - f(x)$ and $\nabla : f(x) \mapsto f(x) - f(x - 1)$ on the space of polynomials of degree at most n over \mathbb{Q} .

Problem 8.25 For a polynomial $f = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{k}[x]$ and a matrix $A \in \text{Mat}_n(\mathbb{k})$, we put $f(A) \stackrel{\text{def}}{=} a_0A^n + a_1A^{n-1} + \cdots + a_{n-1}A + a_nE$ and

²⁷See Sect. 8.1.3 on p. 175.

²⁸See [Problem 7.13](#) on p. 170.

write $\mathbb{k}[A] \subset \text{Mat}_n(\mathbb{k})$ for the image of the evaluation map $\text{ev}_A : \mathbb{k}[x] \rightarrow \text{Mat}_n(\mathbb{k})$, $f \mapsto f(A)$. Recall that the *minimal polynomial* $\mu_A \in \mathbb{k}[x]$ of A is the monic generator of the principal ideal $\ker \text{ev}_A \subset \mathbb{k}[x]$.

- (a) Find a matrix $A \in \text{Mat}_2(\mathbb{Z})$ such that $\mu_A(x) = x^2 - 2$ and show that $\mathbb{Q}[A]$ is a field.
- (b) Find a matrix $A \in \text{Mat}_2(\mathbb{R})$ such that $\mathbb{R}[A] \simeq \mathbb{C}$ and explicitly describe all $a, b, c, d \in \mathbb{R}$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}[A]$.
- (c) Find the minimal polynomial of the matrix

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -a_n \\ 1 & 0 & \dots & 0 & -a_{n-1} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_2 \\ 0 & \dots & 0 & 1 & -a_1 \end{pmatrix}.$$

- (d) For a diagonal matrix $A \in \text{Mat}_n(\mathbb{k})$ with distinct diagonal elements, show that $\mathbb{k}[A] = \{X \in \text{Mat}_n(\mathbb{k}) \mid AX = XA\}$.
- (e*) Show that $\dim \mathbb{k}[A] \leq n$ for all $A \in \text{Mat}_n(\mathbb{k})$.

Chapter 9

Determinants

9.1 Volume Forms

9.1.1 Volume of an n -Dimensional Parallelepiped

Let V be a vector space of dimension n over a field \mathbb{k} . We are going to define the *volume* of a parallelepiped whose edges from some base vertex are n vectors v_1, v_2, \dots, v_n as in Fig. 9.1. Such a volume is a function

$$\omega : V \times V \times \cdots \times V \rightarrow \mathbb{k}, \quad v_1, v_2, \dots, v_n \mapsto \omega(v_1, v_2, \dots, v_n). \quad (9.1)$$

Fig. 9.1 Parallelepiped

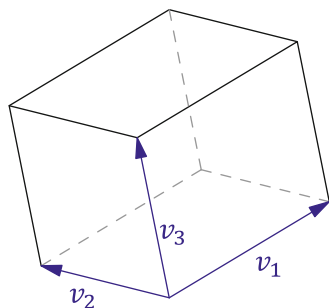
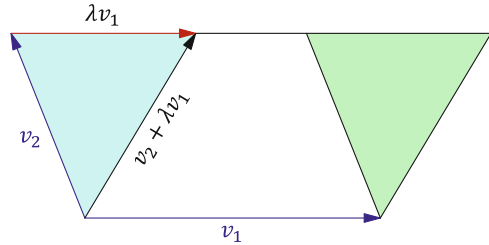


Fig. 9.2 Parallel shift

Geometric intuition imposes two natural restrictions.

First, the volume should not change its value when the parallelepiped undergoes a parallel shift of opposite $(n-1)$ -dimensional faces with respect to each other along some edge parallel to both faces as in Fig. 9.2. Drawn there is the projection of the parallelepiped on the 2-dimensional plane spanned by edge v_2 joining the shifted faces and edge v_1 providing the direction of the shift. The projection goes along the $(n-2)$ -dimensional faces complementary to the target plane of the projection. All these faces are mapped to the vertices of the parallelogram in Fig. 9.2. The parallel shift in question replaces v_2 by $v_2 + \lambda v_1$. Since the prism cut from the left is attached back from the right, the total volume of the parallelepiped remains unchanged.

Second, at least for $\mathbb{k} = \mathbb{Q}, \mathbb{R}$ and positive λ , multiplication of any edge by λ leads to multiplication of the volume by λ . We would like to extrapolate this homogeneity property uniformly to arbitrary fields \mathbb{k} and all $\lambda \in \mathbb{k}$. Writing these geometric constraints algebraically, we come to the following definition.

Definition 9.1 A function of n vectors $\omega : V \times V \times \cdots \times V \rightarrow \mathbb{k}$ is called an *n -dimensional volume form* on an n -dimensional vector space V if it possesses the following two properties (all dotted arguments remain unchanged in both formulas):

- (1) $\omega(\dots, v_i + \lambda v_j, \dots, v_j, \dots) = \omega(\dots, v_i, \dots, v_j, \dots)$ for all $i \neq j$ and all $\lambda \in \mathbb{k}$.
- (2) $\omega(\dots, \lambda v_i, \dots) = \lambda \omega(\dots, v_i, \dots)$ for all i and all $\lambda \in \mathbb{k}$.

Lemma 9.1 Every volume form vanishes on linearly related v_1, v_2, \dots, v_n ; every volume form is linear in each argument,

$$\omega(\dots, \lambda v + \mu w, \dots) = \lambda \omega(\dots, v, \dots) + \mu \omega(\dots, w, \dots); \quad (9.2)$$

and every volume form alternates sign under transpositions of arguments:

$$\omega(\dots, v, \dots, w, \dots) = -\omega(\dots, w, \dots, v, \dots). \quad (9.3)$$

Proof If vectors v_1, v_2, \dots, v_n are linearly related, then one of them is a linear combination of the others, say $v_1 = \lambda_2 v_2 + \cdots + \lambda_n v_n$. Then by the first property

of a volume form,

$$\begin{aligned}\omega(v_1, v_2, \dots, v_n) &= \omega(v_1 - \lambda_2 v_2 - \dots - \lambda_n v_n, v_2, \dots, v_n) \\ &= \omega(0, v_2, \dots, v_n) = \omega(0 \cdot 0, v_2, \dots, v_n) \\ &= 0 \cdot \omega(0, v_2, \dots, v_n) = 0.\end{aligned}$$

The proof of (9.2) splits into two cases. If the arguments in each term on the right-hand side are linearly related, then the arguments on the left-hand side are linearly related too, and both sides of (9.2) vanish. Therefore, we can assume without loss of generality that the arguments of the first term on the right hand-side form a basis of V . Then a vector w is expressed through this basis as $w = \varrho v + u$, where u lies in the linear span of the remaining $(n - 1)$ arguments. The first property of a volume form allows us to rewrite the left-hand side of (9.2) as $\omega(\dots, \lambda v + \mu w, \dots) = \omega(\dots, (\lambda + \mu \varrho)v + \mu u, \dots) = \omega(\dots, (\lambda + \mu \varrho)v, \dots)$ and the second term on the right-hand side as $\mu \omega(\dots, w, \dots) = \mu \omega(\dots, \varrho v + u, \dots) = \mu \omega(\dots, \varrho v, \dots)$. Hence the whole right-hand side equals $\lambda \omega(\dots, v, \dots) + \mu \omega(\dots, \varrho v, \dots) = (\lambda + \mu \varrho) \omega(\dots, v, \dots)$ and coincides with the left-hand side. The equality (9.3) follows from the linearity and the vanishing property already proven,

$$0 = \omega(\dots, v+w, \dots, v+w, \dots) = \omega(\dots, v, \dots, w, \dots) + \omega(\dots, w, \dots, v, \dots),$$

because

$$\omega(\dots, v, \dots, v, \dots) = \omega(\dots, w, \dots, w, \dots) = 0. \quad \square$$

9.1.2 Skew-Symmetric Multilinear Forms

Definition 9.2 Let V be an arbitrary module over a commutative ring K . A Map $\omega : V \times V \times \dots \times V \rightarrow K$ is called a *skew-symmetric multilinear¹ form* if it is linear in each argument and vanishes if some arguments coincide. For example, the 2×2 determinant $\det(v_1, v_2)$ considered in Example 6.4 on p. 125 is a bilinear skew-symmetric form on \mathbb{k}^2 .

Example 9.1 (Volume Form) A volume form on an n -dimensional vector space V is skew-symmetric n -linear by Lemma 9.1. Conversely, every skew-symmetric multilinear form of n arguments satisfies both properties from Definition 9.1 on p. 206 and therefore produces a volume form on V . Indeed, the second property is just a

¹Or m -linear if the number of arguments m needs to be indicated explicitly.

part of linearity, and the first property follows from linearity and skew-symmetry:

$$\begin{aligned}\omega(\dots, v_i + \lambda v_j, \dots, v_j, \dots) \\ &= \omega(\dots, v_i, \dots, v_j, \dots) + \lambda \omega(\dots, v_j, \dots, v_j, \dots) \\ &= \omega(\dots, v_i, \dots, v_j, \dots) .\end{aligned}$$

Remark 9.1 (Sign Alternation vs. Skew-Symmetry) The above proof of equality (9.3) shows in fact that every skew-symmetric multilinear form ω alternates sign under transpositions of arguments, i.e., satisfies

$$\omega(\dots, v, \dots, w, \dots) = -\omega(\dots, w, \dots, v, \dots).$$

Conversely, the substitution $w = v$ transforms the sign alternation condition to $2\omega(\dots, v, \dots, v, \dots) = 0$, which implies skew-symmetry if $2 = 1 + 1$ is not a zero divisor in K . Note that for $\text{char } K = 2$, the sign alternation means the same as the invariance under transpositions of arguments, whereas the skew-symmetry adds an extra nontrivial constraint to this invariance.

9.2 Digression on Parities of Permutations

Let us treat permutations $g = (g_1, g_2, \dots, g_n)$ of an ordered collection $(1, 2, \dots, n)$ as bijective maps

$$g : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}, \quad i \mapsto g_i.$$

These maps form the transformation group $S_n = \text{Aut}(\{1, 2, \dots, n\})$ discussed in Example 1.7 on p. 13. The composition fg of maps $f, g \in S_n$ takes i to $f(g(i))$. For example, the permutation $f = (2, 4, 3, 5, 1) \in S_5$ is performed by the map $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 3$, $4 \mapsto 5$, $5 \mapsto 1$. Two of its compositions with the permutation $g = (3, 2, 1, 5, 4)$ are $fg = (3, 4, 2, 1, 5)$ and $gf = (2, 5, 1, 4, 3)$.

We write s_{ij} for the permutation that swaps i and j and leaves all the other numbers fixed. The permutations s_{ij} are called *transpositions*.

Exercise 9.1 Prove that every permutation is a composition of transpositions.

We say that a permutation g is *even* (respectively *odd*) if g is the composition of an even (respectively odd) number of transpositions. Note that the factorization of g as a composition of transpositions is not unique. For example, even one transposition $s_{13} = (3, 2, 1) \in S_3$ can be written in three essentially different ways: $s_{13} = s_{12}s_{23}s_{12} = s_{23}s_{12}s_{23}$. Nevertheless, the parity of g remains the same for all factorizations. We verify this by giving another definition of parity independent of factorization.

For $g \in S_n$, a pair of increasing integers (i, j) in the range $1 \leq i < j \leq n$ is called an *inversion* of g if $g(i) > g(j)$. Therefore, each $g \in S_n$ decomposes the set of all $n(n-1)/2$ pairs (i, j) into two disjoint parts: inversions and noninversions. The total number of inversions is called the *inversion number* of g . We denote it by $I(g)$.

Lemma 9.2 *For each transposition s_{ij} and arbitrary $g \in S_n$, the inversion numbers $I(g)$ and $I(gs_{ij})$ have opposite parities.*

Proof Let $i < j$. Then the permutations

$$\begin{aligned} g &= (g_1, \dots, g_{i-1}, \mathbf{g_i}, g_{i+1}, \dots, g_{j-1}, \mathbf{g_j}, g_{j+1}, \dots, g_n), \\ gs_{ij} &= (g_1, \dots, g_{i-1}, \mathbf{g_j}, g_{i+1}, \dots, g_{j-1}, \mathbf{g_i}, g_{j+1}, \dots, g_n), \end{aligned} \quad (9.4)$$

differ from each other by swapping the elements $g_i = g(i)$ and $g_j = g(j)$ at the i th and j th positions. The pairs of opposite inversion status² with respect to these two permutations are exhausted by (i, j) and the pairs (i, m) , (m, j) with $i < m < j$. Thus $|I(g) - I(gs_{ij})| = 1 + 2(j - i - 1)$. \square

Corollary 9.1 (Sign of a Permutation) *There exists a unique map*

$$\text{sgn} : S_n \rightarrow \{+1, -1\}$$

such that $\text{sgn}(\text{Id}) = 1$, $\text{sgn}(s_{ij}) = -1$ for every transposition s_{ij} , and

$$\text{sgn}(fg) = \text{sgn}(f) \cdot \text{sgn}(g)$$

for all $f, g \in S_n$. It is defined by $\text{sgn}(g) = (-1)^{I(g)}$ and equals $+1$ if g is even, and -1 if g is odd.

Proof If $g \in S_n$ is a composition of k transpositions, then $(-1)^{I(g)} = (-1)^k$ by Lemma 9.2. \square

Example 9.2 (Thread Rule) The parity of the inversion number can be determined geometrically as follows. Align the numbers $1, 2, \dots, n$ and g_1, g_2, \dots, g_n in two rows and join equal numbers by smooth curves (threads) lying inside the rectangle with vertices $1, n, g_n, g_1$ and having only simple double crossings³ as in Fig. 9.3. Then the total number of intersections of threads has the same parity as $I(g)$. This method of computation of $\text{sgn } g$ is known as the *thread rule*.

²Inversions of one permutation and noninversions of the other.

³That is, at each intersection point, only two threads cross, and they have different tangents at this point.

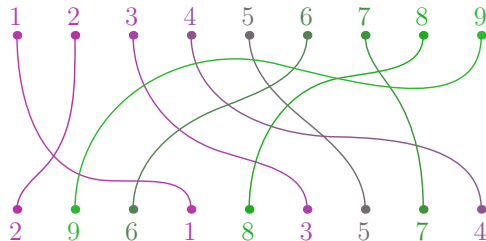


Fig. 9.3 $\text{sgn}(2, 9, 6, 1, 8, 3, 5, 7, 4) = +1$ (18 intersections)

Exercise 9.2 Convince yourself that the thread rule is correct and use it to show that the *shuffle permutation* $(i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_m)$, where $i_1 < i_2 < \dots < i_k$, $j_1 < j_2 < \dots < j_m$, has sign $(-1)^{|I| + \frac{1}{2}k(k+1)}$, where $|I| \stackrel{\text{def}}{=} \sum_v i_v$ is the *weight* of the multi-index I .

9.3 Determinants

Theorem 9.1 For a commutative ring K with unit there exists a unique, up to a constant factor, nonzero skew-symmetric n -linear form ω on the coordinate module K^n . Its value on an arbitrary collection of vectors $\mathbf{v} = (v_1, v_2, \dots, v_n)$, which is expressed through the standard basis $\mathbf{e} = (e_1, e_2, \dots, e_n)$ of K^n as⁴ $\mathbf{v} = \mathbf{e} \cdot C_{\mathbf{ev}}$, where $C_{\mathbf{ev}} = (c_{ij}) \in \text{Mat}_n(K)$, is

$$\omega(v_1, v_2, \dots, v_n) = \omega(e_1, e_2, \dots, e_n) \cdot \det(c_{ij}), \text{ where} \quad (9.5)$$

$$\det(c_{ij}) \stackrel{\text{def}}{=} \sum_{g \in S_n} \text{sgn}(g_1, g_2, \dots, g_n) \cdot c_{g_1 1} c_{g_2 2} \cdots c_{g_n n}$$

(the summation is over all permutations $g = (g_1, g_2, \dots, g_n) \in S_n$).

Definition 9.3 The function $\det(c_{ij})$ in the bottom row of (9.5) is called the *determinant* of the square matrix (c_{ij}) . A matrix C is called *degenerate* if $\det C = 0$. Otherwise, C is called *nondegenerate*.

⁴Recall that the j th column of the transition matrix C is formed by the coordinates of the vector v_j in the standard basis \mathbf{e} .

Proof (of Theorem 9.1) Let us substitute $v_j = \sum_{i=1}^n e_i \cdot c_{ij}$ in $\omega(v_1, v_2, \dots, v_m)$. By the multilinearity of ω , we get

$$\begin{aligned} \omega(v_1, v_2, \dots, v_n) &= \omega\left(\sum_{i_1} e_{i_1} c_{i_1 1}, \sum_{i_2} e_{i_2} c_{i_2 2}, \dots, \sum_{i_n} e_{i_n} c_{i_n n}\right) \\ &= \omega(e_{i_1}, e_{i_2}, \dots, e_{i_n}) \cdot \sum_{i_1 i_2 \dots i_n} c_{i_1 1} \cdot c_{i_2 2} \cdots c_{i_n n}. \end{aligned}$$

By the skew-symmetry of ω , the nonzero summands in the latter sum are only those with distinct indices (i_1, i_2, \dots, i_n) . Such indices are exactly the permutations of $(1, 2, \dots, n)$. Thus,

$$\omega(e_{i_1}, e_{i_2}, \dots, e_{i_n}) = \begin{cases} +\omega(e_1, e_2, \dots, e_n) & \text{for even permutations } (i_1, i_2, \dots, i_n), \\ -\omega(e_1, e_2, \dots, e_n) & \text{for odd permutations } (i_1, i_2, \dots, i_n). \end{cases}$$

This forces every skew-symmetric n -linear form ω on K^n to be computed by formula (9.5). Therefore, such a nonzero form, if it exists, is unique up to the constant factor $\omega(e_1, e_2, \dots, e_n)$. To prove the existence, let us define ω by $\omega(v_1, v_2, \dots, v_n) \stackrel{\text{def}}{=} \det C_{ev}$. We have to check that this function is multilinear, skew-symmetric, and does not vanish identically. This will be done in Proposition 9.1 below after we have developed some properties of determinants. \square

9.3.1 Basic Properties of Determinants

The computational procedure encoded by the formula

$$\det C \stackrel{\text{def}}{=} \sum_{g \in S_n} \text{sgn}(g) \cdot c_{g_1 1} c_{g_2 2} \cdots c_{g_n n} \quad (9.6)$$

prescribes the listing of all n -tuples of matrix elements such that each n -tuple contains exactly one element of each row and exactly one element of each column. Every such n -tuple can be viewed as the graph of the one-to-one correspondence between rows and columns. Associated with such a correspondence are two permutations of the set $\{1, 2, \dots, n\}$: the first takes i to the number of the column corresponding to the i th row; the second takes i to the number of the row corresponding to the i th column. These two permutations are inverse to each other and therefore have the same sign.

Exercise 9.3 Verify that inverse permutations have the same parity.

We attach this sign to the n -tuple of matrix elements that is the graph of the correspondence. Then we multiply the elements in each n -tuple, and sum all these $n!$

products with the attached signs. For 2×2 and 3×3 determinants, this computation gives

$$\det \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = c_{11}c_{22} - c_{12}c_{21}, \quad (9.7)$$

$$\det \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = c_{11}c_{22}c_{33} + c_{13}c_{21}c_{32} + c_{12}c_{23}c_{31} \\ - c_{11}c_{23}c_{32} - c_{13}c_{22}c_{31} - c_{12}c_{21}c_{33}. \quad (9.8)$$

(In the second expansion, the first three summands correspond to the identity and two cyclic permutations, and the latter three summands correspond to the transpositions.)

Exercise 9.4 Verify that $\det E = 1$.

Since rows and columns play completely symmetric roles in the computation just described, we conclude that a matrix and its transpose⁵ have equal determinants:

$$\det C = \sum_{g \in S_n} \operatorname{sgn}(g) \cdot c_{g_1 1} c_{g_2 2} \cdots c_{g_n n} = \sum_{g \in S_n} \operatorname{sgn}(g) \cdot c_{1 g_1} c_{2 g_2} \cdots c_{n g_n} = \det C^t. \quad (9.9)$$

Proposition 9.1 Write v_1, v_2, \dots, v_n for the columns of a matrix $C \in \operatorname{Mat}_n(K)$ and consider them as vectors in K^n . Then the function $\det(v_1, v_2, \dots, v_n) \stackrel{\text{def}}{=} \det C$ is linear in each argument and skew-symmetric.

Proof Each of the $n!$ products in the expansion of $\det C$ contains exactly one factor taken from the j th column of C . Hence, $\det C$ is linear in v_j . To prove skew-symmetry, let $v_i = v_j$ and collect pairs of products corresponding to the pairs of permutations g and gs_{ij} , where s_{ij} is the transposition of i with j . Since $c_{g_i i} = c_{g_j j}$ and $c_{g_j j} = c_{g_i i}$, whereas $\operatorname{sgn}(g) = -\operatorname{sgn}(gs_{ij})$, the products in every such pair cancel each other:

$$\operatorname{sgn}(g) \cdot c_{g_1 1} \cdots c_{g_i i} \cdots c_{g_j j} \cdots c_{g_n n} + \operatorname{sgn}(gs_{ij}) \cdot c_{g_1 1} \cdots c_{g_j i} \cdots c_{g_i j} \cdots c_{g_n n} = 0.$$

Thus $\det(C) = 0$ in this case. \square

Since by [Exercise 9.4](#), $\det(v_1, v_2, \dots, v_n)$ is a nonzero function of v_1, v_2, \dots, v_n , [Proposition 9.1](#) finishes the proof of [Theorem 9.1](#). The equality $\det C = \det C^t$ allows us to reformulate [Proposition 9.1](#) in terms of rows.

⁵Recall that a matrix $C = (c_{ij})$ and its transpose $C^t = (c'_{ij})$ have $c'_{ij} = c_{ji}$.

Corollary 9.2 *Considered as a function of the matrix rows, the determinant is skew-symmetric and linear in each row.*

Corollary 9.3 *Every finite-dimensional vector space V possesses a unique, up to proportionality, nonzero volume form ω . If some basis (e_1, e_2, \dots, e_n) in V is fixed and the form ω is normalized by the condition*

$$\omega(e_1, e_2, \dots, e_n) = 1,$$

then the volume of an arbitrary collection of vectors

$$(v_1, v_2, \dots, v_n) = (e_1, e_2, \dots, e_n)C_{ev}$$

is equal to the determinant of the transition matrix: $\omega(v_1, v_2, \dots, v_n) = \det C_{ev}$.

Exercise 9.5 Show that $\det C = 0$ for every $C \in \text{Mat}_n(\mathbb{k})$ such that $\text{rk } C < n$, where \mathbb{k} is a field.

Proposition 9.2 $\det(AB) = \det(A) \cdot \det(B)$ for every $A, B \in \text{Mat}_n(K)$, where K is any commutative ring.

Proof Consider the difference $\det(AB) - \det(A) \cdot \det(B)$ as a polynomial with integer coefficients in $2n^2$ variables a_{ij} and b_{ij} . It is sufficient to check that it is the zero polynomial.

Exercise 9.6 Let \mathbb{k} be an infinite field. Show that the polynomial $f \in \mathbb{k}[x_1, x_2, \dots, x_m]$ is zero if and only if it assumes the value zero, $f(p_1, p_2, \dots, p_m) = 0 \in \mathbb{k}$, for every point $(p_1, p_2, \dots, p_m) \in \mathbb{k}^m$.

Therefore, to verify the identity $\det(AB) = \det(A) \cdot \det(B)$ in the ring of polynomials in the matrix elements it is enough to prove the proposition for all matrices with elements in \mathbb{Q} . Write $v_1, v_2, \dots, v_n \in \mathbb{Q}^n$ for the columns of A . If they are linearly related, then the dimension of their linear span is less than n . Since the columns of AB are linear combinations of columns of A , the ranks of both matrices A and AB are less than n , and $\det A = \det AB = 0$ by [Exercise 9.5](#). Thus $\det AB = \det A \det B$ in this case. Now assume that the vectors $\mathbf{v} = (v_1, v_2, \dots, v_n)$ form a basis of \mathbb{Q}^n and write $\mathbf{e} = (e_1, e_2, \dots, e_n)$ for the standard basis. Consider two volume forms $\omega_{\mathbf{e}}$ and $\omega_{\mathbf{v}}$ on \mathbb{Q}^n uniquely defined by $\omega_{\mathbf{e}}(e_1, e_2, \dots, e_n) = 1$ and $\omega_{\mathbf{v}}(v_1, v_2, \dots, v_n) = 1$ respectively. By [Corollary 9.3](#), they are proportional with coefficient $\omega_{\mathbf{e}}(v_1, v_2, \dots, v_n) = \det A$:

$$\omega_{\mathbf{e}} = \det(A) \cdot \omega_{\mathbf{v}}. \quad (9.10)$$

Let $w_1, w_2, \dots, w_n \in \mathbb{Q}^n$ be those vectors whose coordinate columns in the basis \mathbf{v} are the columns of the matrix B . Then $(w_1, w_2, \dots, w_n) = (v_1, v_2, \dots, v_n) \cdot B = (e_1, e_2, \dots, e_n) \cdot AB$. Evaluating both sides of [\(9.10\)](#) on the vectors w_1, w_2, \dots, w_n ,

we get $\omega_e(w_1, w_2, \dots, w_n) = \det(AB)$ and $\omega_v(w_1, w_2, \dots, w_n) = \det(B)$ by Corollary 9.3. Therefore, $\det AB = \det A \det B$ for linearly independent v_1, v_2, \dots, v_n as well. \square

Corollary 9.4 $\det(AB) = \det(BA)$ for every pair of square matrices $A, B \in \text{Mat}_n(K)$ over a commutative ring K .

9.3.2 Determinant of a Linear Endomorphism

Let V be a vector space of dimension n , and ω an arbitrary nonzero volume form on V . Every linear endomorphism $F : V \rightarrow V$ makes another volume form $\omega_F(v_1, v_2, \dots, v_n) \stackrel{\text{def}}{=} \omega(Fv_1, Fv_2, \dots, Fv_n)$ from the form ω .

Exercise 9.7 Verify that ω_F is multilinear and skew-symmetric.

By Corollary 9.3, the form ω_F is proportional to ω . Hence, the ratio of their values on a basis e_1, e_2, \dots, e_n of V does not depend on the choice of basis. Since this ratio is

$$\begin{aligned} \frac{\omega(Fe_1, Fe_2, \dots, Fe_n)}{\omega(e_1, e_2, \dots, e_n)} &= \frac{\omega((e_1, e_2, \dots, e_n) \cdot F_e)}{\omega(e_1, e_2, \dots, e_n)} = \frac{\omega(e_1, e_2, \dots, e_n) \cdot \det F_e}{\omega(e_1, e_2, \dots, e_n)} \\ &= \det F_e, \end{aligned}$$

where F_e is the matrix of F in the basis e , the determinant $\det F_e$ is the same for all bases e in V . It is called the *determinant* of the operator F and is denoted by $\det F$. Under the action of F on V , the volumes of all parallelepipeds are multiplied by $\det F$ regardless of what volume form is used:

$$\omega(Fv_1, Fv_2, \dots, Fv_n) = \det F \cdot \omega(v_1, v_2, \dots, v_n)$$

for an arbitrary volume form ω on V and collection of $n = \dim V$ vectors $v_i \in V$. By Proposition 9.2, $\det FG = \det F \det G$ for all $F, G \in \text{End } V$. Therefore, the endomorphisms of determinant 1, that is, the volume-preserving endomorphisms, form a subgroup in the general linear group $\text{GL}(V)$. This group is called the *special linear group* and is denoted by $\text{SL}(V) \subset \text{GL}(V)$.

Exercise 9.8 Show that every linear endomorphism of determinant 1 is invertible and the inverse map also has determinant 1.

The special linear group of the coordinate space \mathbb{k}^n consists of $n \times n$ matrices of determinant 1 and is denoted by $\text{SL}_n(\mathbb{k}) \subset \text{GL}_n(\mathbb{k})$.

9.4 Grassmannian Polynomials

9.4.1 Polynomials in Skew-Commuting Variables

A useful tool for handling determinants over a commutative ring K is the ring of *Grassmannian polynomials* in the skew-commuting variables $\xi_1, \xi_2, \dots, \xi_n$ with coefficients in K . It is denoted by $K\langle \xi_1, \xi_2, \dots, \xi_n \rangle$ and defined in the same way as the usual polynomial ring $\mathbb{K}[x_1, x_2, \dots, x_n]$. The only difference is that the Grassmannian variables *anticommute* instead of commute, that is, they satisfy the relations

$$\forall i, j \quad \xi_i \wedge \xi_j = -\xi_j \wedge \xi_i \quad \text{and} \quad \forall i \quad \xi_i \wedge \xi_i = 0, \quad (9.11)$$

where the symbol \wedge stands for the skew-commutative multiplication of Grassmannian variables in order to prevent confusion with the commutative multiplication of variables in a usual polynomial ring. If $1 + 1$ does not divide zero in K , then the latter relation $\xi_i \wedge \xi_i = 0$ in (9.11) follows from the former written for $i = j$. However, if $1 + 1 = 0$, then the first relation in (9.11) says that the variables commute, whereas the second postulates the actual difference between the Grassmannian polynomials and the usual ones. It follows from (9.11) that every nonzero Grassmannian monomial is at most linear in each variable and up to a sign equals $\xi_{i_1} \wedge \xi_{i_2} \wedge \dots \wedge \xi_{i_m}$ for some $i_1 < i_2 < \dots < i_m$. Thus, $K\langle \xi_1, \xi_2, \dots, \xi_n \rangle$ is a free K -module with a basis formed by the monomials

$$\xi_I \stackrel{\text{def}}{=} \xi_{i_1} \wedge \xi_{i_2} \wedge \dots \wedge \xi_{i_m} \quad (9.12)$$

numbered by all collections $I = (i_1, i_2, \dots, i_m)$, where $1 \leq i_1 < i_2 < \dots < i_m \leq n$. Every permutation of variables multiplies such a monomial by the sign of the permutation:

$$\forall g \in S_m \quad \xi_{i_{g(1)}} \wedge \xi_{i_{g(2)}} \wedge \dots \wedge \xi_{i_{g(m)}} = \text{sgn}(g) \cdot \xi_{i_1} \wedge \xi_{i_2} \wedge \dots \wedge \xi_{i_m}. \quad (9.13)$$

Grassmannian products of basic monomials (9.12) are expressed through those monomials as

$$\xi_I \wedge \xi_J = \begin{cases} \text{sgn}(i_1, i_2, \dots, i_m, j_1, j_2, \dots, j_k) \cdot \xi_{I \sqcup J} & \text{for } I \cap J = \emptyset, \\ 0 & \text{for } I \cap J \neq \emptyset, \end{cases} \quad (9.14)$$

where $\text{sgn}(i_1, i_2, \dots, i_m, j_1, j_2, \dots, j_k) = (-1)^{\frac{1}{2}m(m+1) + \sum i_v}$ by [Exercise 9.2](#).

We write $\Lambda^m K^n \subset K\langle \xi_1, \xi_2, \dots, \xi_n \rangle$ for the K -submodule of homogeneous Grassmannian polynomials of degree m . It is free of rank $\binom{n}{m}$. The entire ring of Grassmannian polynomials splits into the finite direct sum

$$K\langle \xi_1, \xi_2, \dots, \xi_n \rangle = \bigoplus_{m=0}^n \Lambda^m K^n, \quad (9.15)$$

where $\Lambda^k K^n \wedge \Lambda^m K^n \subset \Lambda^{k+m} K^n$. Therefore, in contrast with the usual polynomials, the ring $K\langle \xi_1, \xi_2, \dots, \xi_n \rangle$ is a free K -module of *finite* rank 2^n . Note that the components $\Lambda^0 K^n$ and $\Lambda^n K^n$ of minimum and maximum degree in the decomposition (9.15) both have rank 1. The first of them is generated by the zero-degree monomial $\xi_\emptyset \stackrel{\text{def}}{=} 1$, which is the unit of $K\langle \xi_1, \xi_2, \dots, \xi_n \rangle$. The second is generated by the highest-degree monomial $\xi_{(1,2,\dots,n)} = \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n$, which is annihilated under Grassmannian multiplication by every monomial of positive degree.

Exercise 9.9 Check that Grassmannian monomials commute by the rule

$$\begin{aligned} (\xi_{i_1} \wedge \xi_{i_2} \wedge \dots \wedge \xi_{i_k}) \wedge (\xi_{j_1} \wedge \xi_{j_2} \wedge \dots \wedge \xi_{j_m}) \\ = (-1)^{km} (\xi_{j_1} \wedge \xi_{j_2} \wedge \dots \wedge \xi_{j_m}) \wedge (\xi_{i_1} \wedge \xi_{i_2} \wedge \dots \wedge \xi_{i_k}). \end{aligned}$$

The exercise implies that multiplication of homogeneous Grassmannian polynomials f, g satisfies the *Koszul sign rule*

$$f \wedge g = (-1)^{\deg f \deg g} g \wedge f. \quad (9.16)$$

In particular, each homogeneous Grassmannian polynomial of even degree lies in the *center* of the Grassmannian polynomial ring

$$Z(K\langle \xi_1, \xi_2, \dots, \xi_n \rangle) \stackrel{\text{def}}{=} \{f \mid \forall g, f \wedge g = g \wedge f\}.$$

Exercise 9.10 Find a basis of $Z(K\langle \xi_1, \xi_2, \dots, \xi_n \rangle)$ over K .

9.4.2 Linear Change of Grassmannian Variables

Let the homogeneous linear forms $\eta_1, \eta_2, \dots, \eta_k \in \Lambda^1 K^n$ be expressed linearly through the homogeneous linear forms $\zeta_1, \zeta_2, \dots, \zeta_n \in \Lambda^1 K^n$ by means of the transition matrix $C \in \text{Mat}_{n \times k}(K)$, that is,

$$(\eta_1, \eta_2, \dots, \eta_k) = (\zeta_1, \zeta_2, \dots, \zeta_n) \cdot C.$$

Then the degree- m monomials $\eta_J = \eta_{j_1} \wedge \eta_{j_2} \wedge \cdots \wedge \eta_{j_m}$ are linearly expressed through the monomials $\zeta_I = \zeta_{i_1} \wedge \zeta_{i_2} \wedge \cdots \wedge \zeta_{i_m}$ as follows:

$$\begin{aligned} \eta_J &= \eta_{j_1} \wedge \eta_{j_2} \wedge \cdots \wedge \eta_{j_m} = \left(\sum_{i_1} \zeta_{i_1} c_{i_1 j_1} \right) \wedge \left(\sum_{i_2} \zeta_{i_2} c_{i_2 j_2} \right) \wedge \cdots \wedge \left(\sum_{i_m} \zeta_{i_m} c_{i_m j_m} \right) \\ &= \sum_{1 \leq i_1 < i_2 < \cdots < i_m \leq n} \zeta_{i_1} \wedge \zeta_{i_2} \wedge \cdots \wedge \zeta_{i_m} \cdot \sum_{g \in S_m} \text{sgn}(g) c_{i_{g(1)} j_1} c_{i_{g(2)} j_2} \cdots c_{i_{g(m)} j_m} \\ &= \sum_I \zeta_I \cdot c_{IJ}, \end{aligned}$$

where the latter summation is over all collections $I = (i_1, i_2, \dots, i_m)$ of m strictly increasing indices and $c_{IJ} \stackrel{\text{def}}{=} \det C_{IJ}$ denotes the determinant of the $m \times m$ submatrix $C_{IJ} \subset C$, which consists of those c_{ij} with $i \in I, j \in J$. This determinant is called the IJ th minor of order m in C . Thus, the IJ th element of the transition matrix from η_J to ζ_I is equal to the IJ th minor of the transition matrix from η to ζ .

9.5 Laplace Relations

For a collection of strictly increasing indices

$$J = (j_1, j_2, \dots, j_m), \quad 1 \leq j_1 < j_2 < \cdots < j_m \leq n,$$

let us put $\deg J \stackrel{\text{def}}{=} m$, $|J| \stackrel{\text{def}}{=} j_1 + j_2 + \cdots + j_m$, and write $\bar{J} = (\bar{j}_1, \bar{j}_2, \dots, \bar{j}_{n-m}) = \{1, 2, \dots, n\} \setminus J$ for the complementary collection of increasing indices, which has $\deg \bar{J} = n - m$. Associated with every square matrix $A \in \text{Mat}_n(K)$ are n homogeneous linear forms $\alpha_1, \alpha_2, \dots, \alpha_n \in \Lambda^1 K^n$ such that A is the transition matrix from them to the basic Grassmannian varieties $\xi_1, \xi_2, \dots, \xi_n$, i.e., $(\alpha_1, \alpha_2, \dots, \alpha_n) = (\xi_1, \xi_2, \dots, \xi_n) \cdot A$ or, in the most expanded form,

$$\alpha_j = \xi_1 \cdot a_{1j} + \xi_2 \cdot a_{2j} + \cdots + \xi_n \cdot a_{nj}, \quad 1 \leq j \leq n. \quad (9.17)$$

For a pair of multi-indices I, J of the same length $\deg I = \deg J = m$, consider the Grassmannian monomials $\alpha_J = \alpha_{j_1} \wedge \alpha_{j_2} \wedge \cdots \wedge \alpha_{j_m}$ and $\alpha_{\bar{J}} = \alpha_{\bar{i}_1} \wedge \alpha_{\bar{i}_2} \wedge \cdots \wedge \alpha_{\bar{i}_{n-m}}$ of complementary degrees m and $n-m$. By formula (9.14) on p. 215, their product is

$$\alpha_J \wedge \alpha_{\bar{J}} = \begin{cases} (-1)^{|J|+m(m+1)/2} \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n & \text{for } I = J, \\ 0 & \text{for } I \neq J. \end{cases} \quad (9.18)$$

As we have seen in Sect. 9.4.2, the left-hand side is expanded through $\xi_1, \xi_2, \dots, \xi_n$ as

$$\left(\sum_M \xi_M a_{MJ} \right) \wedge \left(\sum_L \xi_L a_{LI} \right) = (-1)^{m(m+1)/2} \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n \sum_M (-1)^{|M|} a_{MJ} a_{\overline{MI}},$$

where M runs through all the increasing multi-indices of degree $\deg M = m$. The right-hand side of (9.18) vanishes for $I \neq J$ and equals

$$(-1)^{m(m+1)/2+|J|} \det A \cdot \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n$$

for $I = J$. Thus, for any two collections J, I of m columns in a square matrix A , the following *Laplace relations* hold:

$$\sum_M (-1)^{|M|+|J|} a_{MJ} a_{\overline{MI}} = \begin{cases} \det A & \text{for } I = J, \\ 0 & \text{for } I \neq J, \end{cases} \quad (9.19)$$

where the summation is over all collections M of m rows in the matrix A .

For $I = J$, the equality (9.19) expresses $\det A$ through the m th-degree minors a_{MJ} situated in m fixed columns of A numbered by J and their *complementary minors* $a_{\overline{MI}}$ of degree $(n-m)$. The latter are equal to the determinants of the matrix obtained from A by removing all rows and columns containing the minor a_{MJ} . The resulting formula is known as the *cofactor expansion* for the determinant:

$$\det A = \sum_M (-1)^{|M|+|J|} a_{MJ} a_{\overline{MI}}. \quad (9.20)$$

The quantity $(-1)^{|M|+|J|} a_{\overline{MI}}$ is called the *algebraic complement* (or *cofactor*) of the minor a_{MJ} .

For $I \neq J$, the relation (9.19) up to sign looks like

$$\sum_M (-1)^{|M|+|J|} a_{MJ} a_{\overline{MI}} = 0. \quad (9.21)$$

In other words, if the minors a_{MJ} in (9.20) are multiplied by the cofactors complementary to the minors a_{MI} situated in the other collection of columns $I \neq J$, then the resulting sum vanishes.

Exercise 9.11 Prove the transposed version of Laplace's relations

$$\sum_M (-1)^{|I|+|M|} a_{JM} a_{\overline{MI}} = \begin{cases} \det A & \text{for } I = J, \\ 0 & \text{for } I \neq J. \end{cases} \quad (9.22)$$

Let us number all increasing multi-indices I of degree m in some order by integers from 1 to $\binom{n}{m}$. Then we number all complementary increasing multi-indices by the

same integers in such a way that all complementary pairs I, \bar{I} get the same numbers. Write \mathcal{A}_m and \mathcal{A}_m^\vee for the $\binom{n}{m} \times \binom{n}{m}$ matrices whose IJ th elements are equal to a_{IJ} and $a_{IJ}^\vee = (-1)^{|J|+|I|}a_{\bar{I}\bar{J}}$ respectively.⁶ In terms of these matrices, the Laplace relations (9.19), (9.22) are collected in two matrix equalities

$$\mathcal{A}_m^\vee \cdot \mathcal{A}_m = \det A \cdot \mathcal{E} = \mathcal{A}_m \cdot \mathcal{A}_m^\vee, \quad (9.23)$$

where \mathcal{E} means the identity matrix of size $\binom{n}{m} \times \binom{n}{m}$. Therefore, the matrices $\mathcal{A}_m, \mathcal{A}_m^\vee$ commute and are “almost inverse” to each other.

Example 9.3 (Determinant of a Matrix Pencil) Given two square matrices $A, B \in \text{Mat}_n(K)$, consider two commuting scalar variables x, y and form the matrix $x \cdot A + y \cdot B$ with elements $xa_{ij} + yb_{ij} \in K[x, y]$. Its determinant $\det(x \cdot A + y \cdot B)$ is a homogeneous polynomial of degree n in x, y . We are going to show that the coefficient of $x^m y^{n-m}$ in this polynomial equals

$$\sum_{IJ} (-1)^{|I|+|J|} a_{IJ} b_{\bar{I}\bar{J}} = \text{tr}(\mathcal{A}_m \mathcal{B}_m^\vee), \quad (9.24)$$

where the left summation runs through all increasing multi-indices $I, J \subset \{1, 2, \dots, n\}$ of degree $\deg I = \deg J = m$. Consider two collections of homogeneous linear forms

$$(\alpha_1, \alpha_2, \dots, \alpha_n) = (\xi_1, \xi_2, \dots, \xi_n) \cdot A \quad \text{and} \quad (\beta_1, \beta_2, \dots, \beta_n) = (\xi_1, \xi_2, \dots, \xi_n) \cdot B$$

in the Grassmannian polynomial ring $K[x, y]\langle \xi_1, \xi_2, \dots, \xi_n \rangle$. Then

$$(x\alpha_1 + y\beta_1) \wedge (x\alpha_2 + y\beta_2) \wedge \dots \wedge (x\alpha_n + y\beta_n) = \det(xA + yB) \cdot \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n.$$

Multiplying out the left-hand side, we get the monomial $x^m y^{n-m}$ when we choose the first summand within some m factors, say numbered by i_1, i_2, \dots, i_m , and choose the second summand within the remaining $(n-m)$ factors. Such a choice contributes the summand

$$\begin{aligned} & \text{sgn}(i_1, i_2, \dots, i_m, \bar{i}_1, \bar{i}_2, \dots, \bar{i}_{n-m}) \cdot \alpha_{i_1} \wedge \alpha_{i_2} \wedge \dots \wedge \alpha_{i_m} \wedge \beta_{\bar{i}_1} \wedge \beta_{\bar{i}_2} \wedge \dots \wedge \beta_{\bar{i}_{n-m}} \\ &= (-1)^{m(m+1)/2+|I|} \alpha_I \wedge \beta_{\bar{I}} = (-1)^{m(m+1)/2+|I|} \left(\sum_J \xi_J a_{IJ} \right) \wedge \left(\sum_M \xi_M b_{M\bar{I}} \right) \\ &= (-1)^{m(m+1)/2+|I|} \sum_{JM} a_{IJ} \cdot b_{M\bar{I}} \cdot \xi_J \wedge \xi_M \\ &= \left(\sum_J (-1)^{|I|+|J|} a_{IJ} \cdot b_{\bar{I}\bar{J}} \right) \cdot \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n \end{aligned}$$

in the resulting coefficient of $x^m y^{n-m}$. The sum of all these contributions, coming from all increasing multi-indices $I = (i_1, i_2, \dots, i_m)$, is equal to (9.24).

⁶Note that we swap indices I, J on the right-hand side of the latter formula.

Example 9.4 (Principal Minors and Trace) For $x = 1$, $y = t$, $B = E$, formula (9.24) gives the following expansion:

$$\begin{aligned}\det(tE + A) &= t^n + \sum_{m=1}^n t^{n-m} \cdot \sum_{\#I=m} a_{II} \\ &= t^n + t^{n-1} \cdot \sum_i a_{ii} + t^{n-1} \cdot \sum_{i < j} (a_{ii}a_{jj} - a_{ij}a_{ji}) + \cdots + t \cdot \sum_i a_{\bar{ii}} + \det A,\end{aligned}$$

where the coefficient of t^{n-m} is equal to the sum of all the degree- m minors in A whose main diagonal sits within the main diagonal of A . All such minors are called *principal*. For example, the coefficient of t^{n-1} is the trace

$$\operatorname{tr}(A) \stackrel{\text{def}}{=} \sum_{i=1}^n a_{ii}. \quad (9.25)$$

Note that $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B)$ and $\operatorname{tr}(AB) = \sum_{ij} a_{ij}b_{ji} = \operatorname{tr}(BA)$.

9.6 Adjunct Matrix

9.6.1 Row and Column Cofactor Expansions

For $m = 1$, the Laplace relations (9.23) deal with collections $I = (i)$, $J = (j)$, which consist of just one index. In this case, the minors $a_{IJ} = a_{ij}$ become the matrix elements, and therefore, $\mathcal{A}_1 = A$ in (9.23). The second matrix \mathcal{A}_1^\vee in (9.23) is called the *adjunct matrix* of A and is denoted by A^\vee . It has the same size as A and is formed by the cofactors of the transposed elements in A :

$$a_{ij}^\vee \stackrel{\text{def}}{=} (-1)^{i+j} a_{\bar{j}i}. \quad (9.26)$$

The minor $a_{\bar{j}i}$ is equal to the determinant of the matrix obtained from A by removing the j th row and i th column. It is often denoted by A_{ji} . The first Laplace relation (9.20) for $m = 1$ gives the expansion

$$\det A = \sum_{i=1}^n (-1)^{i+j} a_{ij} a_{\bar{j}i} = \sum_{i=1}^n (-1)^{i+j} a_{ij} A_{ji}, \quad (9.27)$$

called the *cofactor expansion of $\det A$ through the j th column*. Its transposed version (9.22),

$$\det A = \sum_{j=1}^n (-1)^{i+j} a_{ij} a_{\bar{j}i} = \sum_{j=1}^n (-1)^{i+j} a_{ij} A_{ij}, \quad (9.28)$$

is called the *cofactor expansion of the determinant through the i th row*. For example, the cofactor expansion of a 3×3 determinant through the first column looks like

$$\begin{aligned} \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \\ = a_{11} (a_{22}a_{33} - a_{23}a_{32}) - a_{21} (a_{12}a_{33} - a_{13}a_{32}) + a_{31} (a_{12}a_{23} - a_{13}a_{22}) . \end{aligned}$$

The matrix relations (9.23) for $m = 1$ become

$$A \cdot A^\vee = A^\vee \cdot A = \det(A) \cdot E = \begin{pmatrix} \det(A) & & 0 \\ & \ddots & \\ 0 & & \det(A) \end{pmatrix} . \quad (9.29)$$

9.6.2 Matrix Inversion

Proposition 9.3 *Over a commutative ring K with unit, a matrix $A \in \text{Mat}_n(K)$ is invertible if and only if $\det A$ is invertible in K . In this case, $A^{-1} = A^\vee / \det A$.*

Proof If A is invertible, then the matrix equality $AA^{-1} = E$ forces $\det(A) \det(A^{-1}) = 1$ in K . Therefore, $\det A$ is invertible in K . Conversely, if $\det A$ is invertible, then formula (9.29) says that $A^{-1} = A^\vee / \det A$. \square

Exercise 9.12 Prove that for every finite-dimensional vector space V , the following properties of a linear endomorphism $F : V \rightarrow V$ are equivalent: **(a)** $\ker F = 0$, **(b)** $\text{im } F = V$, **(c)** $\det F \neq 0$.

Example 9.5 For 2×2 and 3×3 matrices of determinant 1, we get

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} &= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \\ \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}^{-1} &= \begin{pmatrix} (a_{22}a_{33} - a_{23}a_{32}) & -(a_{12}a_{33} - a_{13}a_{31}) & (a_{12}a_{23} - a_{13}a_{22}) \\ -(a_{21}a_{33} - a_{23}a_{31}) & (a_{11}a_{33} - a_{13}a_{31}) & -(a_{11}a_{23} - a_{13}a_{21}) \\ (a_{21}a_{32} - a_{22}a_{31}) & -(a_{11}a_{32} - a_{12}a_{32}) & (a_{11}a_{22} - a_{12}a_{21}) \end{pmatrix}. \end{aligned}$$

For matrices of arbitrary invertible determinant, all matrix elements on the right-hand sides must be divided by this determinant.

9.6.3 Cayley–Hamilton Identity

Let us introduce n^2 variables a_{ij} , $1 \leq i, j \leq n$, and write $K = \mathbb{Z}[a_{ij}]_{1 \leq i, j \leq n}$ for the usual commutative polynomial ring in these variables with integer coefficients. Then $A = (a_{ij})$ is a matrix from $\text{Mat}_n(K)$. Let t be another variable commuting with all a_{ij} . Consider the matrix $tE - A \in \text{Mat}_n(K[t])$. Its determinant $\chi_A(t) \stackrel{\text{def}}{=} \det(tE - A)$, which is a polynomial in t with coefficients in K , is called the *characteristic polynomial* of the matrix A . Recall⁷ that every polynomial $f \in K[t]$ can be evaluated at any matrix $M \in \text{Mat}_n(K)$ by the substitution⁸ $t \leftrightarrow M$. In particular, we can evaluate $\chi_A(t)$ for $t = A$.

Theorem 9.2 (Cayley–Hamilton Identity) $\chi_A(A) = 0$ in $\text{Mat}_n(K)$.

Proof Formula (9.29) written in the matrix algebra $\text{Mat}_n(K[t])$ for the matrix $tE - A$ says that

$$\det(tE - A) \cdot E = (tE - A) \cdot (tE - A)^\vee. \quad (9.30)$$

Each $B \in \text{Mat}_n(K[t])$ can be written as $t^m B_m + t^{m-1} B_{m-1} + \cdots + t B_1 + B_0$ for some constant matrices $B_i \in \text{Mat}_n(K)$. Such an expanded version of (9.30) looks like

$$t^n E + s_1(A) \cdot t^{n-1} E + \cdots + s_{n-1}(A) \cdot t E + s_0(A) \cdot E = (tE - A) (t^m A_m^\vee + \cdots + t A_1^\vee + A_0^\vee),$$

where $t^m A_m^\vee + \cdots + t A_1^\vee + A_0^\vee = (tE - A)^\vee$ and $s_i(A) \in K$ mean the coefficients of the characteristic polynomial $\chi_A(t)$. Substituting $t = A$ we get the required equality $\chi_A(A) = 0$. \square

Example 9.6 Each 2×2 matrix A satisfies the quadratic equation⁹

$$A^2 - \text{tr}(A) \cdot A + \det(A) \cdot E = 0.$$

Each 3×3 matrix A satisfies the cubic equation

$$A^3 - \text{tr}(A) \cdot A^2 + s_2(A) \cdot A - \det(A) \cdot E = 0,$$

where

$$s_2 \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = (a_{11}a_{22} - a_{12}a_{21}) + (a_{11}a_{33} - a_{13}a_{31}) + (a_{22}a_{33} - a_{23}a_{32})$$

is the sum of the principal 2×2 minors.

⁷See Sect. 8.1.3 on p. 175.

⁸Under this substitution, the degree-zero monomial t^0 evaluates to $M^0 = E$.

⁹Compare with formula (8.5) on p. 179.

Corollary 9.5 Every matrix $A \in \text{Mat}_n(\mathbb{K})$ is algebraic over \mathbb{K} and has degree at most n . The minimal polynomial of A divides the characteristic polynomial $\chi_A(t) = \det(tE - A)$. \square

9.6.4 Cramer's Rules

Consider the coordinate module K^n over a commutative ring K with unit and write vectors $v \in K^n$ as columns. For n vectors $v_1, v_2, \dots, v_n \in K^n$ expressed through the standard basis as $(v_1, v_2, \dots, v_n) = (e_1, e_2, \dots, e_n) \cdot C$, we put, as usual,

$$\det(v_1, v_2, \dots, v_n) \stackrel{\text{def}}{=} \det C.$$

Proposition 9.4 (Cramer's Rule I) The vectors $v_1, v_2, \dots, v_n \in K^n$ form a basis of K^n if and only if $\det(v_1, v_2, \dots, v_n)$ is invertible in K . In this case, for every vector $w = x_1 v_1 + x_2 v_2 + \dots + x_n v_n$, the coordinates x_i can be computed by Cramer's rule¹⁰:

$$x_i = \frac{\det(v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_n)}{\det(v_1, v_2, \dots, v_n)}. \quad (9.31)$$

Proof We know from Lemma 8.1 on p. 181 that the vectors v_1, v_2, \dots, v_n form a basis of K^n if and only if the transition matrix C from those vectors to the standard basis is invertible.

Exercise 9.13 Convince yourself that the proof of Lemma 8.1 is valid for every free module V over a commutative ring K with unit.

By Proposition 9.3, the invertibility of C is equivalent to the invertibility of $\det C$. This proves the first statement. Now assume that $\det(v_1, v_2, \dots, v_n)$ is invertible and let $w = x_1 v_1 + x_2 v_2 + \dots + x_n v_n$. Then

$$\begin{aligned} \det(v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_n) &= \det(v_1, \dots, v_{i-1}, \sum_v x_v v_v, v_{i+1}, \dots, v_n) \\ &= \sum_v x_v \cdot \det(v_1, \dots, v_{i-1}, v_v, v_{i+1}, \dots, v_n) \\ &= x_i \cdot \det(v_1, \dots, v_{i-1}, v_i, v_{i+1}, \dots, v_n). \end{aligned} \quad \square$$

Corollary 9.6 For every $w \in K^n$ and invertible $A \in \text{Mat}_n(K)$, the linear equation $Ax = w$ in the unknown vector $x \in K^n$ has a unique solution. The coordinates of this solution are given by Cramer's rule (9.31), where $v_1, v_2, \dots, v_n \in K^n$ are the columns of the matrix A .

¹⁰Compare with formula (6.13) on p. 127.

Proof The system $Ax = w$ describes the coefficients of the linear expression $w = \sum v_i x_i$. \square

Proposition 9.5 (Cramer's Rule II) *Given a system of n linear homogeneous equations in $n + 1$ unknowns (x_0, x_1, \dots, x_n) ,*

$$\begin{cases} a_{10}x_0 + a_{11}x_1 + \dots + a_{1n}x_n = 0, \\ a_{20}x_0 + a_{21}x_1 + \dots + a_{2n}x_n = 0, \\ \dots \\ a_{n0}x_0 + a_{n1}x_1 + \dots + a_{nn}x_n = 0, \end{cases} \quad (9.32)$$

we write A_j , where $j = 0, 1, \dots, n$, for the determinant of the $n \times n$ matrix obtained by removing the j th column from the coefficient matrix $A = (a_{ij})$:

$$A_j = \det \begin{pmatrix} a_{1,0} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1,n} \\ a_{2,0} & \dots & a_{2,j-1} & a_{2,j+1} & \dots & a_{2,n} \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ a_{n,0} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{n,n} \end{pmatrix}. \quad (9.33)$$

Then $x_v = (-1)^v A_v$ solves the system.

Proof Let us attach a second copy of the i th row to the top of the matrix A . We get an $(n + 1) \times (n + 1)$ matrix with zero determinant. The cofactor expansion of this determinant through the top row leads to the equality

$$a_{i0}A_0 - a_{i1}A_1 + \dots + (-1)^n a_{in}A_n = 0,$$

which says that $x_v = (-1)^v A_v$ satisfies the i th equation of the system. \square

Corollary 9.7 *Let $K = \mathbb{k}$ be a field. Then equations (9.32) are linearly independent if and only if Cramer's rule II produces a nonzero solution. In this case, all solutions of the system (9.32) are proportional to the Cramer's-rule solution.*

Proof If the rows of A are linearly related, then all A_i are equal to 0. If $\text{rk } A = n$, then by Exercise 8.9 on p. 187, there should be some $n \times n$ submatrix of rank n in A . Then its determinant A_i is nonzero. This proves the first statement. If it holds, then the rows of A span an n -dimensional subspace $U \in \mathbb{k}^{n+1}$. Hence, $\text{Ann}(U) \subset \mathbb{k}^{n+1*}$ is one-dimensional. \square

Example 9.7 The line of intersection of two distinct planes in \mathbb{k}^3 is given by the equations

$$\begin{cases} a_1x + a_2y + a_3z = 0, \\ b_1x + b_2y + b_3z = 0, \end{cases}$$

and is spanned by the vector $(a_2b_3 - a_3b_2, -a_1b_3 + a_3b_1, a_1b_2 - a_2b_1)$.

Problems for Independent Solution to Chap. 9

In all the problems below, we follow our standard defaults: \mathbb{k} means an arbitrary field, K means any commutative ring with unit.

Problem 9.1 Calculate $\text{sgn}(n, (n-1), \dots, 2, 1)$ and $\det \begin{pmatrix} 0 & 1 \\ & \ddots \\ 1 & 0 \end{pmatrix}$.

Problem 9.2 For a $A \in \text{Mat}_n(K)$, $C \in \text{Mat}_m(K)$, and $B \in \text{Mat}_{n \times m}(K)$, show that

$$\det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det A \cdot \det C.$$

Problem 9.3 Show that the determinant of a triangular matrix¹¹ equals the product of its diagonal elements.

Problem 9.4 Let all u_{ij} equal 1 in the square matrix $U = (u_{ij})$. Calculate $\det(U - E)$, where E is the identity matrix.

Problem 9.5 Two rows of a 3×3 matrix are filled with integers such that the greatest common divisor of each row equals 1. Is it always possible to fill the third row to create an integer matrix of determinant 1?

Problem 9.6 Find the total number of (a) 2×2 matrices of given determinant over $\mathbb{F}_p = \mathbb{Z}/(p)$, (b) nondegenerate¹² $n \times n$ matrices over \mathbb{F}_q .

Problem 9.7 (Zolotarev's Proof of Quadratic Reciprocity) For a $a \in \mathbb{F}_p^*$, a permutation of the finite set \mathbb{F}_p is given by $x \mapsto ax$. Show that the sign of this permutation is equal to the Legendre–Jacobi symbol¹³ $\left(\frac{a}{p}\right)$. For prime integers $p, q > 2$, consider two permutations of the finite set $\mathbb{F}_p \times \mathbb{F}_q \simeq \mathbb{Z}/(pq)$ defined by

$$s_p : (x, y) \mapsto (x, x + py) \quad \text{and} \quad s_q : (x, y) \mapsto (qx + y, y).$$

Relate their signs to the values $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$, calculate the sign of the composition $s_p \circ s_q^{-1}$, and deduce the quadratic reciprocity law¹⁴ from these observations.

Problem 9.8 Find the sum of the determinants of all distinct $n \times n$ matrices whose entries are the numbers $1, 2, 3, \dots, n^2$, each appearing exactly once.

Problem 9.9 Consider a 3-diagonal square matrix A such that all elements on the main diagonal and on the next diagonal above equal 1, whereas all elements on

¹¹See Example 8.17 on p. 197.

¹²See Definition 9.3 on p. 210.

¹³See Sect. 3.6.3 on p. 65.

¹⁴See formula (3.23) on p. 66.

the diagonal below the main diagonal equal -1 (all the other elements are zero). Show that $\det(A)$ is among the Fibonacci numbers.¹⁵

Problem 9.10 Given a function $f : \mathbb{N} \times \mathbb{N} \rightarrow K$, write $(f(i, j)) \in \text{Mat}_n(K)$ for the square matrix whose (i, j) th element equals $f(i, j)$. For any two collections of real numbers $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n$ compute (a) $\det(\alpha_i \beta_j)$, (b) $\det(\cos(\alpha_i - \beta_j))$, (c) $\det(\alpha_i^{j-1})$, (d*) $\det(\alpha^{j-i-1 \pmod n})$.

Problem 9.11 Show that for a set X , the functions $f_1, f_2, \dots, f_n : X \rightarrow \mathbb{K}$ are linearly independent in \mathbb{K}^X if and only if there exist points $x_1, x_2, \dots, x_n \in X$ such that $\det(f_i(t_j)) \neq 0$.

Problem 9.12 (Bordered Minors Theorem) Let the matrix $A \in \text{Mat}_{m \times n}(\mathbb{K})$ contain a nondegenerate square $k \times k$ submatrix B such that all $(k+1) \times (k+1)$ submatrices of A containing B are degenerate. Show that $\text{rk } A = k$.

Problem 9.13 (Kirchhoff's Matrix Tree Theorem) For a connected graph Γ with n vertices numbered $1, 2, \dots, n$, consider the square matrix $A = A(\Gamma) = (a_{ij})$ such that each diagonal element a_{ii} equals the number of edges going out of the i th vertex, and each nondiagonal element a_{ij} equals -1 if the i th and j th vertices are joined by some edge, and 0 otherwise. Prove that $\det A = 0$ but each principal cofactor A_{ii} is equal to the number of *spanning trees*¹⁶ of the graph Γ . To begin with, assume that Γ itself is a tree. Then show that Γ is a tree if and only if all A_{ii} are equal to 1 . Then attack the general case.

Problem 9.14 For a square matrix $A \in \text{Mat}_n(\mathbb{K})$, write

$$L_A, R_A, \text{Ad}_A : \text{Mat}_n(\mathbb{K}) \rightarrow \text{Mat}_n(\mathbb{K})$$

for the linear endomorphism sending the matrix $X \in \text{Mat}_n(\mathbb{K})$ to the matrices

$$L_A(X) \stackrel{\text{def}}{=} A \cdot X, \quad R_A(X) \stackrel{\text{def}}{=} X \cdot A, \quad \text{Ad}_A(X) \stackrel{\text{def}}{=} A \cdot X \cdot A^{-1},$$

respectively. Calculate the traces and determinants of these endomorphisms.

Problem 9.15 Write $S^2 \subset \mathbb{K}[x_1, x_2]$ for the subspace of homogeneous quadratic polynomials in $x = (x_1, x_2)$. Associated with every matrix $A \in \text{Mat}_2(\mathbb{K})$ is the linear change of variables

$$F_A : \mathbb{K}[x_1, x_2] \rightarrow \mathbb{K}[x_1, x_2], \quad f(x) \mapsto f(x \cdot A).$$

Show that this change of variables sends S^2 to itself and calculate the trace and determinant of the restricted map

$$F_A|_{S^2} : S^2 \rightarrow S^2.$$

Problem 9.16 (Characteristic Polynomial) Let a linear endomorphism

$$F : V \rightarrow V$$

¹⁵See Example 4.4 on p. 81.

¹⁶Subtrees of Γ containing all the vertices of Γ .

have matrix A in some basis of V . Prove that the characteristic polynomial $\chi_A(t) = \det(tE - A)$ does not depend on the choice of basis.

Problem 9.17 Let $A, B \in \text{Mat}_n(K)$ satisfy the relation $AB = E$. Show that the complementary minors of A, B satisfy the relation $a_{IJ} = (-1)^{|I|+|J|}b_{\overline{J}\overline{I}}$.

Problem 9.18 Calculate all partial derivatives

$$\frac{\partial^k \det(A)}{\partial a_{i_1 j_1} \partial a_{i_2 j_2} \cdots \partial a_{i_k j_k}}.$$

Problem 9.19 (Plücker's Relations) Use the Laplace relations to show that the six numbers A_{ij} , $1 \leq i < j \leq 4$, are the second-degree minors of some 2×4 matrix¹⁷ $A \in \text{Mat}_{2 \times 4}(\mathbb{k})$ if and only if $A_{12}A_{23} - A_{13}A_{24} + A_{14}A_{23} = 0$. Is there some complex 2×4 matrix whose second-degree minors (written in some random order) are (a) $\{2, 3, 4, 5, 6, 7\}$? (b) $\{3, 4, 5, 6, 7, 8\}$? If such matrices exist, write some of them explicitly. If not, explain why.

Problem 9.20 (Antisymmetric Matrices) A square matrix A such that $A^t = -A$ is called *antisymmetric*. Show that every antisymmetric matrix of odd dimension is degenerate. Verify that the determinant of an antisymmetric 2×2 or 4×4 matrix is a perfect square in the ring of polynomials in matrix elements with integer coefficients.

Problem 9.21 Find all a, b, c, φ such that the following matrices are invertible, and explicitly calculate the inverse:

$$(a) \begin{pmatrix} 1 & 1 \\ 1 & a+1 \end{pmatrix}, \quad (b) \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}, \quad (c) \begin{pmatrix} 1 & 0 & c \\ 0 & b & 0 \\ a & 0 & 1 \end{pmatrix}, \quad (d) \begin{pmatrix} 1 & a & 0 \\ 0 & b & 0 \\ 0 & c & 1 \end{pmatrix}.$$

Problem 9.22 (Sylvester's Determinants) Let \mathbb{k} be a field. For two polynomials

$$A(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_{m-1} x + a_m$$

$$B(x) = b_0 x^m + b_1 x^{m-1} + \cdots + b_{m-1} x + b_m$$

in $\mathbb{k}[x]$ such that $a_0 b_0 \neq 0$ and $m \geq n$, write $P_d \subset \mathbb{k}[x]$ for the subspace of polynomials of degree at most d and consider linear map

$$\varphi : P_{n-1} \oplus P_{m-1} \rightarrow P_{m+n-1}, \quad (f, g) \mapsto Ag + Bf.$$

- (a) Check that φ is \mathbb{k} -linear and write its matrix in the standard monomial bases.
 (b) Show that φ is bijective if and only if $\text{GCD}(A, B) = 1$.

¹⁷Meaning that A_{ij} equals the determinant of the submatrix formed by the i th and j th columns.

- (c) For each $v = 0, 1, 2, \dots$ write d_v for the determinant of the $(m + n - 2v) \times (m + n - 2v)$ matrix constructed from the $(m + n) \times (m + n)$ matrix¹⁸

$$\underbrace{\left(\begin{array}{cccccc} a_0 & \dots & \dots & a_{n-1} & a_m & \\ & a_0 & \dots & \dots & a_{n-1} & a_m \\ & & \ddots & & & \ddots \\ & & & a_0 & \dots & \dots & a_{n-1} & a_m \\ & & & & b_0 & \dots & b_{m-1} & b_n \\ & & & & \ddots & \ddots & \ddots & \\ & & & & & \ddots & \ddots & \ddots \\ & & & & & & b_0 & \dots & b_{m-1} & b_n \\ b_0 & \dots & b_{m-1} & b_n & & & & & & \end{array} \right)}_{m+n} \left. \vphantom{\begin{pmatrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{pmatrix}} \right\} \begin{matrix} n \\ m \end{matrix} \quad (9.34)$$

by removing v sequential exterior bordering perimeters. Show that $\deg \text{GCD}(A, B)$ coincides with the index of the first nonzero element in the sequence d_0, d_1, d_2, \dots .

- (d) **(Resultant)** In the polynomial ring $\mathbb{Z}[t, a_0, b_0, \alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$ put

$$A(t) = a_0 t^m + a_1 t^{m-1} + \dots + a_{m-1} t + a_m \stackrel{\text{def}}{=} a_0 \prod_{i=1}^m (t - \alpha_i),$$

$$B(t) = b_0 t^n + b_1 t^{n-1} + \dots + b_{n-1} t + b_n \stackrel{\text{def}}{=} b_0 \prod_{j=1}^n (t - \beta_j).$$

The quantity $R_{A,B} \stackrel{\text{def}}{=} a_0^n \prod_i B(\alpha_i) = a_0^n b_0^m \prod_{i,j} (\alpha_i - \beta_j) = (-1)^{mn} b_0^m \prod_j A(\beta_j)$ considered as an element of the ring $\mathbb{Z}[a_0, a_1, \dots, a_m, b_0, b_1, \dots, b_n]$ is called the *resultant* of the polynomials A, B . Show that $R_{A,B}$ equals the determinant of the matrix¹⁹ (9.34) and can be represented as

$$R_{A,B} = f(t) \cdot A(t) + g(t) \cdot B(t)$$

for appropriate $f, g \in \mathbb{Z}[t]$. For all $A, B \in \mathbb{k}[t]$, show that²⁰ $R_{A,B} \in \mathbb{k}$ vanishes if and only if A and B are not coprime in $\mathbb{k}[x]$.

¹⁸All elements outside the strips shown in (9.34) equal zero.

¹⁹Called *Sylvester's determinant*.

²⁰The number $R_{A,B} \in \mathbb{k}$ is the result of evaluation of $R_{A,B} \in \mathbb{Z}[a_0, a_1, \dots, a_m, b_0, b_1, \dots, b_n]$ on the coefficients of given polynomials $A, B \in \mathbb{k}[t]$.

Chapter 10

Euclidean Spaces

10.1 Inner Product

10.1.1 Euclidean Structure

Let V be a vector space over the field of real numbers \mathbb{R} . An *inner product* on V is a function $V \times V \rightarrow \mathbb{R}$ sending a pair of vectors $u, w \in V$ to a number $(u, w) \in \mathbb{R}$ such that $(u, w) = (w, u)$ for all $u, w \in V$, $(v, v) > 0$ for all $v \neq 0$, and

$$\begin{aligned} &(\lambda_1 u_1 + \lambda_2 u_2, \mu_1 w_1 + \mu_2 w_2) \\ &= \lambda_1 \mu_1 (u_1, w_1) + \lambda_1 \mu_2 (u_1, w_2) + \lambda_2 \mu_1 (u_2, w_1) + \lambda_2 \mu_2 (u_2, w_2), \end{aligned}$$

for all $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{R}$ and all $u_1, u_2, w_1, w_2 \in V$. The first condition is called *symmetry*, the second, *positivity*, and the third, *bilinearity*.¹ A real vector space V equipped with an inner product is called a *Euclidean* vector space. An inner product on a Euclidean space is also called a *Euclidean structure*.

Example 10.1 (Coordinate Space) Let V be the coordinate space \mathbb{R}^n . For $u = (x_1, x_2, \dots, x_n)$, $w = (y_1, y_2, \dots, y_n)$ in V put

$$(u, w) \stackrel{\text{def}}{=} x_1 y_1 + x_2 y_2 + \dots + x_n y_n. \quad (10.1)$$

This function is obviously bilinear, symmetric, and positive. The inner product (10.1) is called the *standard* Euclidean structure on \mathbb{R}^n .

¹Bilinearity means that the inner product is linear in each argument while the other argument is fixed.

Example 10.2 (Continuous Functions) Let V be the space of continuous real-valued functions on some segment $[a, b] \subset \mathbb{R}$. The inner product of functions $f, g \in V$ is defined by

$$(f, g) \stackrel{\text{def}}{=} \int_a^b f(x)g(x) dx. \quad (10.2)$$

Exercise 10.1 Check that (f, g) is bilinear and positive.

If functions $[a, b] \rightarrow \mathbb{R}$ are thought of as elements of an infinite-dimensional coordinate vector space $\mathbb{R}^{[a,b]}$, then the inner product (10.2) appears as a generalization of the standard Euclidean structure (10.1). There are various such generalizations in several directions. One can consider other classes of integrable functions instead of the continuous. The only constraint imposed by positivity is

$$f \not\equiv 0 \Rightarrow \int_a^b f^2(x) dx > 0.$$

Conversely, the inner product (10.2) can be restricted to some subspaces in V , e.g., on the space of polynomials of degree at most n . On the other hand, one can change the notion of integral, e.g., integrate with some weight. Finally, one can consider other integration domains instead of the segment.

10.1.2 Length of a Vector

Associated with a Euclidean structure on V is a *length function*

$$V \rightarrow \mathbb{R}_{\geq 0}, \quad v \mapsto |v| \stackrel{\text{def}}{=} \sqrt{(v, v)}.$$

Note that $|v| > 0$ for all $v \neq 0$ and $|\lambda v| = |\lambda| \cdot |v|$ for all $\lambda \in \mathbb{R}$, $v \in V$. The inner product $V \times V \rightarrow \mathbb{R}$ is uniquely recovered from the length function as

$$(u, w) = (|u + w|^2 - |u|^2 - |w|^2) / 2 = (|u + w|^2 - |u - w|^2) / 4. \quad (10.3)$$

10.1.3 Orthogonality

Vectors u, w in a Euclidean space are called *orthogonal*² if $(u, w) = 0$. For every pair of orthogonal vectors a, b , the length of the vector $c = b - a$, which joins the

²Or *perpendicular*.

heads of a, b (see Fig. 10.1), satisfies the *Pythagorean theorem*

$$|c|^2 = (c, c) = (b - a, b - a) = (a, a) + (b, b) = |a|^2 + |b|^2.$$

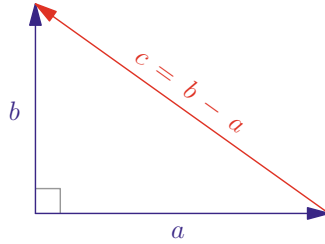


Fig. 10.1 Right triangle

A collection of mutually orthogonal vectors e_1, e_2, \dots, e_k is called an *orthogonal collection*. If all vectors in an orthogonal collection have length 1, the collection is called *orthonormal*. Associated with every orthonormal basis e_1, e_2, \dots, e_n of V is an isomorphism

$$V \simeq \mathbb{R}^n, \quad x_1 e_1 + x_2 e_2 + \dots + x_n e_n \mapsto (x_1, x_2, \dots, x_n),$$

which identifies the inner product on V with the standard one on \mathbb{R}^n described in Example 10.1. Indeed, the orthonormality relations

$$(e_i, e_j) = \begin{cases} 1 & \text{for } i = j, \\ 0 & \text{for } i \neq j, \end{cases} \quad (10.4)$$

force $(\sum_i x_i e_i, \sum_j y_j e_j) = \sum_{ij} x_i y_j (e_i, e_j) = \sum_{ij} x_i y_j$. For an orthonormal basis, the i th coordinate $x_i = x_i(v)$ of a vector $v = \sum_i x_i e_i$ is equal to the inner product (v, e_i) , because

$$(v, e_j) = \left(\sum_i x_i e_i, e_j \right) = \sum_i x_i (e_i, e_j) = x_j.$$

The length of a vector can be computed by the generalized Pythagorean theorem:

$$|v|^2 = (v, v) = \sum_i x_i^2.$$

10.2 Gramians

10.2.1 Gram Matrices

In Euclidean space, associated with any two finite sequences of vectors

$$\mathbf{u} = (u_1, u_2, \dots, u_m) \quad \text{and} \quad \mathbf{w} = (w_1, w_2, \dots, w_k) \quad (10.5)$$

is the $m \times n$ matrix of reciprocal inner products between the vectors

$$G_{\mathbf{u}\mathbf{w}} \stackrel{\text{def}}{=} ((u_i, w_j)) \quad (10.6)$$

called the *Gram matrix* or just *Gramian* of collections \mathbf{u}, \mathbf{w} . For $\mathbf{w} = \mathbf{u}$, the Gramian becomes the inner product table $((u_i, u_j))$ of vectors $\mathbf{u} = (u_1, u_2, \dots, u_m)$. We write $G_{\mathbf{u}}$ instead of $G_{\mathbf{u}\mathbf{u}}$ in this case. The Gram matrix $G_{\mathbf{u}}$ is *symmetric*, i.e., $G_{\mathbf{u}}^t = G_{\mathbf{u}}$. Its determinant $\Gamma_{\mathbf{u}} \stackrel{\text{def}}{=} \det G_{\mathbf{u}}$ is called the *Gram determinant* of the vectors \mathbf{u} . The vectors $\mathbf{e} = (e_1, e_2, \dots, e_m)$ are orthonormal if and only if $G_{\mathbf{e}} = E$. In this case, $\Gamma_{\mathbf{e}} = 1$.

Matrix computations with Gramians are simplified if we allow the multiplication of matrices whose elements are vectors by treating the product of two vectors as an inner product: $uv \stackrel{\text{def}}{=} (v, u) \in \mathbb{R}$. Then the Gramian $G_{\mathbf{u}\mathbf{w}}$ of two collections of vectors (10.5) becomes the product of a column matrix \mathbf{u}^t and a row matrix \mathbf{w} :

$$G_{\mathbf{u}\mathbf{w}} = \mathbf{u}^t \mathbf{w}. \quad (10.7)$$

Let $\mathbf{u} = \mathbf{e}C_{\mathbf{e}\mathbf{u}}$, $\mathbf{w} = \mathbf{f}C_{\mathbf{f}\mathbf{w}}$ be linearly expressed in terms of some other collections of vectors

$$\mathbf{e} = (e_1, e_2, \dots, e_r) \quad \text{and} \quad \mathbf{f} = (f_1, f_2, \dots, f_s).$$

Substitution of these expressions in (10.7) leads to $G_{\mathbf{u}\mathbf{w}} = \mathbf{u}^t \mathbf{w} = (\mathbf{e}C_{\mathbf{e}\mathbf{u}})^t \mathbf{f}C_{\mathbf{f}\mathbf{w}} = C_{\mathbf{e}\mathbf{u}}^t \mathbf{e}^t \mathbf{f} C_{\mathbf{f}\mathbf{w}} = C_{\mathbf{e}\mathbf{u}}^t G_{\mathbf{e}\mathbf{f}} C_{\mathbf{f}\mathbf{w}}$. We conclude that Gramians $G_{\mathbf{u}\mathbf{w}}$ and $G_{\mathbf{e}\mathbf{f}}$ are related as

$$G_{\mathbf{u}\mathbf{w}} = C_{\mathbf{e}\mathbf{u}}^t G_{\mathbf{e}\mathbf{f}} C_{\mathbf{f}\mathbf{w}}. \quad (10.8)$$

Lemma 10.1 *Let $\mathbf{e} = (e_1, e_2, \dots, e_n)$ be an orthonormal basis of a Euclidean space V . Then $\Gamma_{\mathbf{u}} = \det^2 C_{\mathbf{e}\mathbf{u}}$ for every collection of n vectors $\mathbf{u} = (u_1, u_2, \dots, u_n) = \mathbf{e} \cdot C_{\mathbf{e}\mathbf{u}}$.*

Proof Since $G_{\mathbf{u}} = C_{\mathbf{e}\mathbf{u}}^t G_{\mathbf{e}} C_{\mathbf{e}\mathbf{u}} = C_{\mathbf{e}\mathbf{u}}^t E C_{\mathbf{e}\mathbf{u}} = C_{\mathbf{e}\mathbf{u}}^t C_{\mathbf{e}\mathbf{u}}$ and $\det C_{\mathbf{e}\mathbf{u}} = \det C_{\mathbf{e}\mathbf{u}}^t$, we get $\Gamma_{\mathbf{u}} = \det G_{\mathbf{u}} = \det^2 C_{\mathbf{e}\mathbf{u}}$. \square

Proposition 10.2 *For every collection of vectors $\mathbf{u} = (u_1, u_2, \dots, u_m)$, the inequality $\Gamma_{\mathbf{u}} = \det((u_i, u_j)) \geq 0$ holds. It is an equality if and only if the vectors u_1, u_2, \dots, u_m are linearly related.*

Proof Let $\mathbf{e} = (e_1, e_2, \dots, e_k)$ be an orthonormal basis in the linear span of vectors u_1, u_2, \dots, u_m . Then $G_u = C_{eu}^t C_{eu}$. If \mathbf{u} is linearly independent, then \mathbf{u} is also a basis, $k = m$, $\det C_{eu} \neq 0$, and $\Gamma_u = \det^2 C_{eu} > 0$. If \mathbf{u} is linearly related, then $k < m$ and $\text{rk} G_u = \text{rk}(C_{eu}^t C_{eu}) \leq k < m$. Hence $\det G_u = 0$. \square

10.2.2 Euclidean Volume

Let us fix some orthonormal basis $\mathbf{e} = (e_1, e_2, \dots, e_n)$ in a Euclidean space V and write ω for the volume form such that $\omega(e_1, e_2, \dots, e_n) = 1$. Then for every collection of vectors $\mathbf{v} = (v_1, v_2, \dots, v_n)$, we get a remarkable equality:

$$\omega^2(v_1, v_2, \dots, v_n) = \Gamma_{\mathbf{v}}. \quad (10.9)$$

That is, the Gram determinant of every collection of n vectors is the squared volume of the parallelepiped spanned by the vectors, if the volume form is normalized in such a way that the volume of some orthonormal basis is 1. Hence, the absolute value of the volume does not depend on the choice of orthonormal basis used to normalize the volume form. This absolute value is denoted by

$$\text{Vol}(v_1, v_2, \dots, v_n) = |\omega(v_1, v_2, \dots, v_n)| = \sqrt{\Gamma_{\mathbf{v}}} = \sqrt{\det(v_i, v_j)} \quad (10.10)$$

and called the *Euclidean volume* on V . As a byproduct, we get the following corollary.

Corollary 10.2 *All orthonormal bases of a finite-dimensional Euclidean space V have the same absolute value of volume with respect to any volume form on V . Their Euclidean volume equals 1.* \square

10.2.3 Orientation

We say that two orthonormal bases in a Euclidean space V are *cooriented* if they have the same volume with respect to some nonzero volume form on V . Otherwise, the bases are called *contraoriented*. The latter means that their volumes have equal absolute values but opposite signs. It follows from Corollary 10.2 that every two orthonormal bases are either cooriented or contraoriented, and this does not depend on the choice of volume form. Note that the odd permutations of orthonormal basis vectors as well as multiplication of some odd number of vectors by -1 changes the orientation of the basis. Even permutations of basis vectors preserve the orientation of the basis.

10.2.4 Cauchy–Bunyakovsky–Schwarz Inequality

For a collection of two vectors $v, w \in V$, the inequality $\det \begin{pmatrix} (v, v) & (v, w) \\ (w, v) & (w, w) \end{pmatrix} \geq 0$ from Proposition 10.2 can be written as

$$(v, v) \cdot (w, w) \geq (v, w)^2 \quad (10.11)$$

and is known as the *Cauchy–Bunyakovsky–Schwarz inequality*. By Proposition 10.2, it becomes an equality if and only if the vectors v, w are proportional.

For the standard Euclidean structure on \mathbb{R}^n from Example 10.1, the Cauchy–Bunyakovsky–Schwarz inequality (10.11) says that for every two collections of real numbers x_1, x_2, \dots, x_n and y_1, y_2, \dots, y_n , the inequality

$$(x_1^2 + x_2^2 + \dots + x_n^2) \cdot (y_1^2 + y_2^2 + \dots + y_n^2) \geq (x_1 y_1 + x_2 y_2 + \dots + x_n y_n)^2 \quad (10.12)$$

holds, and it is an equality if and only if the collections are proportional.

For continuous functions $f, g : [a, b] \rightarrow \mathbb{R}$ from Example 10.2 we get the integral inequality

$$\left(\int_a^b f^2(x) dx \right) \cdot \left(\int_a^b g^2(x) dx \right) \geq \left(\int_a^b f(x)g(x) dx \right)^2,$$

which is an equality if and only if $f = \lambda g$ for some constant $\lambda \in \mathbb{R}$.

10.3 Duality

10.3.1 Isomorphism $V \simeq V^*$ Provided by Euclidean Structure

A Euclidean structure $V \times V \rightarrow \mathbb{R}$ can be viewed as a perfect pairing between V and V in the sense of Sect. 7.1.4 on p. 160. In particular, it produces a linear map

$$g : V \rightarrow V^*, \quad u \mapsto (*, u), \quad (10.13)$$

sending a vector u to the linear form $g_u : w \mapsto (w, u)$ on V . This map is injective, because for $v \neq 0$, the covector $g_v \in V^*$ takes a nonzero value $g_v(v) = (v, v) > 0$ on the vector $v \in V$. For finite-dimensional V , the injectivity of the linear map (10.13) is equivalent to bijectivity.

Exercise 10.2 Check that the matrix of the linear map (10.13) written in any pair of dual bases e, e^* of V and V^* coincides with the Gram matrix G_e .

Therefore, every linear form $V \rightarrow \mathbb{R}$ on a Euclidean space can be written as an inner product with an appropriate vector uniquely determined by the form. In particular, the coordinate forms $v_1^*, v_2^*, \dots, v_n^* \in V^*$ of any⁴ basis $\mathbf{v} = (v_1, v_2, \dots, v_n)$ in V can be written as inner products with some vectors $v_1^\vee, v_2^\vee, \dots, v_n^\vee \in V$ uniquely determined from the relations

$$(v_i^\vee, v_j) = (v_j, v_i^\vee) = \begin{cases} 0, & \text{for } i \neq j, \\ 1, & \text{for } i = j. \end{cases} \quad (10.14)$$

In the matrix notation introduced in formula (10.7) on p. 233, these relations are written as $\mathbf{v}^t \cdot \mathbf{v}^\vee = E$, where \mathbf{v}^t and \mathbf{v}^\vee mean (v_1, v_2, \dots, v_n) written as a column and $(v_1^\vee, v_2^\vee, \dots, v_n^\vee)$ written as a row. Therefore, the transition matrix $C_{\mathbf{v}\mathbf{v}^\vee}$, which is formed by the coordinate columns of the vectors \mathbf{v}^\vee in the basis \mathbf{v} , satisfies the relation $E = \mathbf{v}^t \cdot \mathbf{v}^\vee = \mathbf{v}^t \cdot \mathbf{v} \cdot C_{\mathbf{v}\mathbf{v}^\vee} = G_{\mathbf{v}} \cdot C_{\mathbf{v}\mathbf{v}^\vee}$. Thus, $C_{\mathbf{v}\mathbf{v}^\vee} = G_{\mathbf{v}}^{-1}$, i.e.,

$$\mathbf{v}^\vee = \mathbf{v} \cdot G_{\mathbf{v}}^{-1}. \quad (10.15)$$

Exercise 10.3 Check that $v_i^{\vee\vee} = v_i$.

The bases $v_1^\vee, v_2^\vee, \dots, v_n^\vee$ and v_1, v_2, \dots, v_n in V are said to be *Euclidean dual* to each other. Every orthonormal basis is Euclidean dual to itself. For the orthogonal basis u_1, u_2, \dots, u_n , the dual basis vectors are $u_i^\vee = u_i/|u_i|^2$. Since the coordinates of every vector $w \in V$ in an arbitrary basis v_1, v_2, \dots, v_n are equal to the inner products with the Euclidean dual basic vectors, we get the equality

$$w = \sum_i (w, v_i^\vee) \cdot v_i. \quad (10.16)$$

Exercise 10.4 Check this assertion by taking the inner product of the both sides with v_i^\vee .

10.3.2 Orthogonal Complement and Orthogonal Projection

Let V be a Euclidean vector space and $U \subset V$ a subspace. The subspace $U^\perp = g^{-1}(\text{Ann}U) = \{w \in V \mid \forall u \in U (u, w) = 0\}$ is called the *orthogonal*⁵ of U . If $\dim V = n < \infty$, then Theorem 7.2 on p. 162 implies that for every integer k in the range $0 \leq k \leq n$, the correspondence $U \rightleftarrows U^\perp$ establishes a bijection between k -dimensional and k -codimensional subspaces in V . This bijection reverses

⁴Not necessarily orthogonal or orthonormal.

⁵Or *orthogonal complement* to U .

the inclusions and possesses the following properties: $U^{\perp\perp} = U$, $(U \cap W)^\perp = U^\perp + W^\perp$, $(U + W)^\perp = U^\perp \cap W^\perp$.

Theorem 10.1 (Orthogonal Decomposition) *Let U be a proper nonzero finite-dimensional subspace of an arbitrary⁶ Euclidean space V . Then*

$$V = U \oplus U^\perp,$$

and for every vector $v \in V$, there exists a unique vector $v_U \in U$ possessing the following equivalent properties:

- (1) $v_U = \pi_U v$, where $\pi_U : V \rightarrow U$ is the projection along U^\perp .
- (2) For every pair of Euclidean dual bases u_1, u_2, \dots, u_k and $u_1^\vee, u_2^\vee, \dots, u_k^\vee$ in U ,

$$v_U = \sum_{i=1}^k (v, u_i^\vee) \cdot u_i. \quad (10.17)$$

- (3) $(v, u) = (v_U, u)$ for all $u \in U$.

- (4) $v - v_U \in U^\perp$.

- (5) For all $u \neq v_U$ in U , the strict inequality $|v - v_U| < |v - u|$ holds.⁷

Proof Let us verify first that properties (2), (3), (4) are equivalent. The equivalence (3) \iff (4) is obvious, because for all $u \in U$, the equalities $(v, u) = (v_U, u)$ and $(v - v_U, u) = 0$ mean the same thing. Since both sides of the equality $(v, u) = (v_U, u)$ in (3) are linear in u , this equality holds for all $u \in U$ if and only if it holds for every basis vector of some basis in U . If $v_U \in U$ satisfies (2) for *some* dual bases of U , then (3) holds for every basis vector u_j^\vee :

$$(v_U, u_j^\vee) = \left(\sum_v (v, u_v^\vee) \cdot u_v, u_j^\vee \right) = (v, u_j^\vee) \cdot (u_j, u_j^\vee) = (v, u_j^\vee).$$

Thus (2) \Rightarrow (3). Conversely, if a vector $v_U \in U$ satisfies (3), then its expression in terms of *every* basis u_1, u_2, \dots, u_k in U by formula (10.16) is (10.17). Therefore, (3) \Rightarrow (2).

Now let us choose some basis in U and *define* the vector v_U by the formula (10.17). Then v_U satisfies (3) and (4) as well. If we perform this for all $v \in V$, we may write every $v \in V$ as $v = v_U + (v - v_U)$, where $v_U \in U$ and $v - v_U \in U^\perp$. Hence, $V = U + U^\perp$. Certainly $U \cap U^\perp = 0$, because every $w \in U \cap U^\perp$ is forced to have $(w, w) = 0$. Therefore, $V = U \oplus U^\perp$ and $v_U = \pi_U v$. This proves the first statement of the theorem as well as the uniqueness of v_U and the equivalence between (1) and (2), (3), (4). It remains to check that for every nonzero vector $w \in U$, the strict inequality $|v - v_U| < |v - (v_U + w)|$ holds. Since both sides

⁶Not necessarily finite-dimensional.

⁷In other words, the minimal distance between the point $v \in \mathbb{A}(V)$ and the points of the affine space $\mathbb{A}(U)$ is achieved at a unique point of $\mathbb{A}(U)$, and this point is v_U .

are positive, it is enough to verify the same inequality between their squares. Since $v - v_U \in U^\perp$, we have $|v - (w + v_U)|^2 = ((v - v_U) - w, (v - v_U) - w) = (v - v_U, v - v_U) + (w, w) = |v - v_U|^2 + |w|^2 > |v - v_U|^2$ as required. \square

Definition 10.1 (Orthogonal Projection) Under the conditions of Sect. 10.3.2, the linear projection $\pi_U : V \rightarrow U$ along U^\perp is called the *orthogonal projection* of V onto U .

Example 10.3 (Euclidean Volume of a Parallelepiped Revisited) Let V be a Euclidean vector space of dimension $\dim V > n$. Consider a collection of $n + 1$ vectors $v, u_1, u_2, \dots, u_n \in V$ and write U for the linear span of the last n vectors u_1, u_2, \dots, u_n . By Theorem 10.1, we can write the first vector v as $v = \pi_U v + h$, where $\pi_U v \in U$ is the orthogonal projection of v on U and $h \in U^\perp$. Note that geometrically, $|h|$ is the distance between the opposite n -dimensional faces parallel to u_1, u_2, \dots, u_n in the $(n + 1)$ -dimensional parallelepiped spanned by v, u_1, u_2, \dots, u_n . Since $\pi_U v$ is a linear combination of vectors u_i , the Euclidean volume of the latter parallelepiped equals

$$\begin{aligned} \text{Vol}(v, u_1, u_2, \dots, u_n) &= |\det(v, u_1, u_2, \dots, u_n)| = |\det(h, u_1, u_2, \dots, u_n)| \\ &= \sqrt{\Gamma_{h, u_1, u_2, \dots, u_n}}. \end{aligned}$$

Expansion of the Gram determinant $\Gamma_{h, u_1, u_2, \dots, u_n}$ in terms of the first column leads to the equality

$$\text{Vol}(v, u_1, u_2, \dots, u_n) = |h| \cdot \text{Vol}(u_1, u_2, \dots, u_n). \quad (10.18)$$

In other words, the Euclidean volume of a parallelepiped equals the Euclidean volume of its codimension-1 hyperface multiplied by the distance between this face and the opposite one.

10.4 Metric Geometry

10.4.1 Euclidean Metric

In this section we deal with the affine space $\mathbb{A}^n = \mathbb{A}(V)$ associated with an n -dimensional Euclidean vector space V . For two points $p, q \in \mathbb{A}(V)$, the length of a vector $\vec{pq} = q - p$ is called the *Euclidean distance* between those points and is denoted by

$$|p, q| \stackrel{\text{def}}{=} |\vec{pq}| = \sqrt{(q - p, q - p)}. \quad (10.19)$$

Recall that a set X is called a *metric space* if it is equipped with a *distance function* $X \times X \rightarrow \mathbb{R}, p, q \mapsto |p, q|$, such that for every triple of points $p, q, r \in X$, the

following properties hold:

$$\begin{aligned}
 |p, q| &= |q, p| && \text{(symmetry),} \\
 |p, q| &\geq 0 && \text{(nonnegativity),} \\
 |p, q| &= 0 \iff p = q && \text{(nonsingularity),} \\
 |p, q| &\leq |p, r| + |r, q| && \text{(triangle inequality).}
 \end{aligned} \tag{10.20}$$

The Euclidean distance (10.19) certainly satisfies the first three properties. The triangle inequality rewritten in terms of vectors asserts that

$$\forall u, w \in V \quad |u| + |w| \geq |u + w|. \tag{10.21}$$

The Cauchy–Bunyakovsky–Schwarz inequality (10.11) forces

$$|u + w|^2 = |u|^2 + |w|^2 + 2(u, w) \leq |u|^2 + |w|^2 + 2|u| \cdot |w| = (|u| + |w|)^2.$$

Hence the triangle inequality (10.21) holds for the Euclidean distance as well. Thus, every affine Euclidean space $\mathbb{A}(V)$ is a metric space, and it inherits all the desirable properties of those spaces known from calculus.

Exercise 10.5 Show that equality is achieved in (10.21) if and only if $w = \lambda u$ for some $\lambda \geq 0$.

Example 10.4 (Distance Between a Point and a Subspace) For a point $a \in \mathbb{A}^n$ and affine subspace $\Pi \subset \mathbb{A}^n$ such that $a \notin \Pi$, Theorem 10.1 says that the minimal distance $|a, p|$ taken over all $p \in \Pi$ is achieved at a unique point $a_\Pi \in \Pi$, which is determined by the orthogonality condition $(\vec{q\bar{p}}, \vec{a\bar{a}_\Pi}) = 0$ for all $q, p \in \Pi$. Such a point $a_\Pi \in \Pi$ is called the *orthogonal projection*⁸ of a . The distance

$$|a, \Pi| \stackrel{\text{def}}{=} |a, a_\Pi| = \min_{p \in \Pi} |a, p|$$

is called the *distance between a and Π* . If $a \in \Pi$, we put $|a, \Pi| = 0$. To compute $|a, \Pi|$, let us fix some point $q \in \Pi$ and write $U \subset V$ for the vectorization of Π centered at q . Then the vector $\vec{q\bar{a}_\Pi} = \pi_U(\vec{q\bar{a}})$ is the orthogonal projection of the vector $v = \vec{q\bar{a}}$ on U . The distance $|a, \Pi| = |v - \pi_U v|$ equals the height of parallelepiped spanned by v and any basis u_1, u_2, \dots, u_k in U . The formula (10.18) on p. 238 expresses this height as the ratio of Gram determinants:

$$|a, \Pi|^2 = \Gamma_{v, u_1, u_2, \dots, u_m} / \Gamma_{u_1, u_2, \dots, u_m}, \tag{10.22}$$

⁸Or the *foot of the perpendicular* drawn from a onto Π .

where $v = \overrightarrow{qa}$, $q \in \Pi$ is an arbitrary point, and the vectors $u_i = \overrightarrow{qp_i}$ form a basis of U , the direction vector space of $\Pi \subset \mathbb{A}^n$.

Example 10.5 (Minimal Distance Method) In practice, the distances between points and affine spaces appear often in the context of minimization. For example, let us find the minimum of the integral

$$\int_0^1 f^2(t) dt$$

over all monic cubic polynomials $f(t) = t^3 + a_1 t^2 + a_2 t + a_3 \in \mathbb{R}[x]$. It equals the distance between the zero polynomial $a = 0$ and the 3-dimensional affine space Π of monic cubic polynomials in the affinization of Euclidean space from Example 10.2 on p. 230 with inner product

$$(f, g) = \int_0^1 f(t) \cdot g(t) dt.$$

Take $q = t^3$ as the origin in Π and use $u_1 = 1$, $u_2 = t$, $u_3 = t^2$ as a basis in the vectorization of Π centered at q . Then $v = \overrightarrow{qa} = -t^3$. Since the inner products of basis vectors are

$$(u_i, u_j) = \int_0^1 t^{i+j-2} dt = (i+j-1)^{-1},$$

the Gram determinant of the basis is

$$\Gamma_{u_1, u_2, u_3} = \det \begin{pmatrix} 1 & 1/2 & 1/3 \\ 1/2 & 1/3 & 1/4 \\ 1/3 & 1/4 & 1/5 \end{pmatrix} = \frac{1}{2160}.$$

The Gram determinant of the collection $(v, u_1, u_2, u_3) = (-t^3, 1, t, t^2)$ is

$$\Gamma_{v, u_1, u_2, u_3} = \det \begin{pmatrix} 1/7 & -1/4 & -1/5 & -1/6 \\ -1/4 & 1 & 1/2 & 1/3 \\ -1/5 & 1/2 & 1/3 & 1/4 \\ -1/6 & 1/3 & 1/4 & 1/5 \end{pmatrix} = \frac{1}{6\,048\,000}.$$

By formula (10.22), the square of the minimum we are looking for is equal to

$$\frac{2160}{6\,048\,000} = \frac{1}{2800}.$$

Exercise 10.6 Find the polynomial $f(t)$ on which the above minimum is achieved and verify the previous answer by explicit evaluation of the integral $\int_0^1 f^2(t) dt$.

Example 10.6 (Equation of a Hyperplane) For every nonzero vector $a \in V$ and $d \in \mathbb{R}$, the inhomogeneous linear equation

$$(a, x) = d \quad (10.23)$$

in the unknown vector $x \in V$ describes an affine hyperplane in $\mathbb{A}(V)$. This hyperplane is perpendicular to the vector a and is shifted the distance $|d|/|a|$ from the origin in the direction of the vector a for $d > 0$ and in the opposite direction for $d < 0$. Indeed, the direction vector space of this hyperplane, which is determined by the homogeneous equation $(a, x) = 0$, is the orthogonal to the 1-dimensional vector space $\mathbb{R} \cdot a$. A particular solution of the inhomogeneous equation (10.23) is provided by the vector $x = d \cdot a/|a|^2$. It is proportional to a and has length $|d|/|a|$. Geometrically, equation (10.23) describes the locus of all points x with prescribed orthogonal projection $\pi_a x = (a, x) \cdot a^\vee = d \cdot a/|a|^2$ on the line $\mathbb{R} \cdot a$ (see Fig. 10.3).

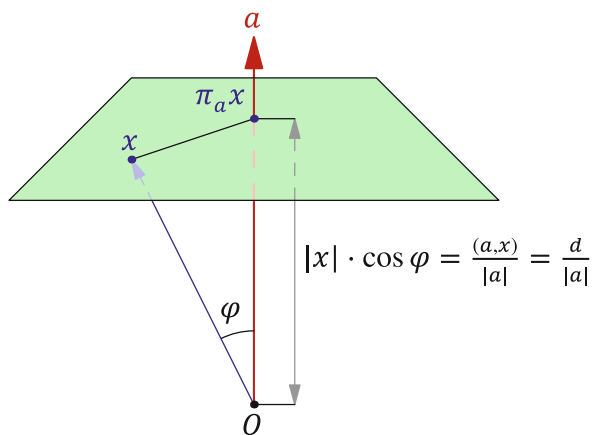


Fig. 10.3 Locus of $x : (a, x) = d$

Exercise 10.7 Check that the distance from a point p to the hyperplane (10.23) is $|d - (a, p)|/|a|$.

Example 10.7 (Equidistant Plane) For two distinct points $a, b \in \mathbb{A}(V)$, their *equidistant* is the locus of all points $x \in \mathbb{A}(V)$ such that $|x, a| = |x, b|$. The latter condition is equivalent to the equality $(a - x, a - x) = (b - x, b - x)$ involving the radius vectors $a, b, x \in V$. The distribution of parentheses and cancellation of quadratic terms turns it into the linear equation $2(b - a, x) = (b, b) - (a, a)$. We

know from Example 10.6 that this equation describes the hyperplane perpendicular to the segment $[a, b]$ and passing through its midpoint $(a + b)/2$.

Exercise 10.8 Check the last claim.

For this reason, the equidistant of a, b is also called the *middle perpendicular* to $[a, b]$.

10.4.2 Angles

The *angle* $\angle(u, w) \in [0, \pi]$ between two nonzero vectors u, w in a Euclidean space V is defined by

$$\cos \angle(u, w) = \frac{(u, w)}{|u| \cdot |w|}. \quad (10.24)$$

The Cauchy–Bunyakovsky–Schwarz inequality⁹ guarantees that the right-hand side belongs to the segment $[-1, 1]$, which is the range of cosine values, and that

$$\cos \angle(u, w) = \pm 1 \iff \frac{w}{|w|} = \pm \frac{u}{|u|}.$$

The angle is symmetric in u, w , and is not changed under the multiplication of vectors by positive scalars. A change of direction of any one vector changes the angle by the contiguous angle: $\angle(u, -w) = \angle(-u, w) = \pi - \angle(u, w)$. Orthogonality of u and w means that $\angle(u, w) = \pi/2$.

If u, w are not collinear, the vectors $e_1 = u/|u|$ and $e_2 = v/|v|$, where $v = w - (w, e_1) \cdot e_1$, form an orthonormal basis e_1, e_2 in the linear span of u, w .

Exercise 10.9 Check that the bases e_1, e_2 and u, w of that linear span are cooriented.

The coefficients of the orthogonal decomposition $w = x_1 e_1 + x_2 e_2$ are

$$x_1 = (w, e_1) = (w, u)/|u| = |w| \cdot \cos \angle(u, w)$$

and $x_2 = (w, e_2) = (w, v)/|v| = ((w, w) - (w, e_1)^2)/|v| = (1 - \cos^2 \angle(u, w)) \cdot |w|^2/|v|$. Since the latter is positive, the equality $x_1^2 + x_2^2 = |w|^2$ forces

$$x_2 = |w| \cdot \sin \angle(u, w).$$

⁹See formula (10.11) on p. 235.

On the other hand, by Cramer's rule,¹⁰ $x_2 = \det(e_1, w) = \det(u, w)/|u|$, where $\det(u, w)$ is the oriented area¹¹ of the parallelogram spanned by u, w . Thus, we get another formula for the angle between u and w :

$$\sin \angle(u, w) = \frac{s(u, w)}{|u| \cdot |w|}, \text{ where } s(u, w) = |\det(u, w)| = \sqrt{\Gamma_{u, w}}. \quad (10.25)$$

In contrast with (10.24), formula (10.25) does not distinguish between acute and obtuse angles.

Example 10.8 (Angle Between a Vector and a Subspace) For every nonzero vector $v \in V$ and vector u running through some subspace $U \subset V$, the angle $\angle(v, u)$ either equals $\pi/2$ for all $u \in U$ or reaches its minimal value over all $u \in U$ exactly on the ray of vectors $\lambda \pi_U v$, $\lambda > 0$. The first case occurs for $v \in U^\perp$. Otherwise, the minimum of $\angle(v, u)$ corresponds to the maximum of

$$\cos(\angle(v, u)) = \frac{(v, u)}{|v| \cdot |u|} = \frac{(\pi_U v, u)}{|v| \cdot |u|} = \frac{1}{|v|} \cdot (\pi_U v, u/|u|).$$

The Cauchy–Bunyakovsky–Schwarz inequality¹² forces the rightmost factor to reach its maximum at the unique unit vector $u/|u|$ that is codirectional with $\pi_U v$. Note that $\angle(v, \pi_U v)$ is acute in this case. We write $\angle(v, U) = \angle(v, \pi_U v)$ for the angle between the vector u and its orthogonal projection on U and call it the *angle between v and U* . This angle can be computed by the formulas¹³

$$\begin{aligned} \cos \angle(v, U) &= |\pi_U v|/|v|, \\ \sin \angle(v, U) &= |v - \pi_U v|/|v| = \sqrt{\Gamma_{v, u_1, u_2, \dots, u_m} / \Gamma_{u_1, u_2, \dots, u_m}} / |v|, \end{aligned} \quad (10.26)$$

where u_1, u_2, \dots, u_m is any basis in U .

Example 10.9 (Angle Between Hyperplanes) Let $\dim V = n \geq 2$. Then for any two hyperplanes $\Pi_1, \Pi_2 \subset \mathbb{A}^n = \mathbb{A}(V)$ with different direction subspaces $W_1, W_2 \subset V$, the codimension $\text{codim}(W_1 \cap W_2)$ is equal to 2. Hence $\Pi_1 \cap \Pi_2$ is a nonempty affine subspace of codimension 2 in \mathbb{A}^n perpendicular to the 2-dimensional affine plane $\mathbb{A}((W_1 \cap W_2)^\perp)$.

Exercise 10.10 Check this.

The latter plane intersects hyperplanes Π_1, Π_2 along two nonparallel lines. The nonobtuse angle between these lines is called the *angle between the hyperplanes*

¹⁰See formula 6.13 on p. 127.

¹¹Normalized by the condition $\det(e_1, e_2) = 1$.

¹²See formula (10.11) on p. 235.

¹³Compare with formula (10.22) on p. 239.

Π_1, Π_2 . We denote it by $\angle(\Pi_1, \Pi_2)$. For parallel hyperplanes having $W_1 = W_2$, we put $\angle(\Pi_1, \Pi_2) \stackrel{\text{def}}{=} 0$. If hyperplanes Π_1, Π_2 are given by the linear equations $(a_1, x) = d_1$ and $(a_2, x) = d_2$ respectively, then $W_i^\perp = \mathbb{R} \cdot a_i$ and the plane $(W_1 \cap W_2)^\perp = W_1^\perp + W_2^\perp$ is spanned by the vectors a_1, a_2 . The intersection lines of this plane with Π_1 and Π_2 are perpendicular to these vectors. Thus,

$$\sin \angle(\Pi_1, \Pi_2) = \sin \angle(a_1, a_2) = \sqrt{\Gamma_{(a_1, a_2)}} / (|a_1| \cdot |a_2|) .$$

10.5 Orthogonal Group

10.5.1 Euclidean Isometries

A linear endomorphism $F : V \rightarrow V$ of a Euclidean vector space V is called *orthogonal*¹⁴ if it preserves lengths, that is, if $|Fv| = |v|$ for all $v \in V$. Formula (10.3) on p. 230 forces every orthogonal map F to preserve all inner products as well, that is, $(Fv, Fw) = (v, w)$ for all $v, w \in V$. Thus, every orthogonal map sends an orthonormal basis to an orthonormal basis. Conversely, if a linear map $F : V \rightarrow V$ takes some basis of V to some vectors with the same Gramian, then F preserves inner products of all vectors and therefore is orthogonal.

An orthogonal map that preserves the Euclidean structure also preserves all geometric quantities derived from it, e.g., angles and Euclidean volume. Preservation of Euclidean volume forces $\det F = \pm 1$. In particular, all orthogonal maps are invertible. Orthogonal maps of determinant $+1$ are called *proper*. Such maps preserve the orientation. Orthogonal maps of determinant -1 are called *improper*. They reverse the orientation.

The set of orthogonal endomorphisms forms a subgroup of the general linear group $\text{GL}(V)$. It is called the *orthogonal group* of V and is denoted by $\text{O}(V) \subset \text{GL}(V)$. The proper orthogonal automorphisms form a subgroup

$$\text{SO}(V) \stackrel{\text{def}}{=} \text{O}(V) \cap \text{SL}(V)$$

in $\text{O}(V)$. It is called the *special orthogonal group* of V .

10.5.2 Orthogonal Matrices

Choose some orthonormal basis $e = (e_1, e_2, \dots, e_n)$ in V and represent all linear maps $F : V \rightarrow V$ by their matrices F_e in this basis. Since $F(e) = e \cdot F_e$, the Gramian $G_{F(e)}$ is equal to $F(e)^t F(e) = F_e^t e^t e F_e = F_e^t G_e F_e = F_e^t F_e$. Therefore, the orthogonality of F , which means $G_{F(e)} = E$, is equivalent to the relation $F_e^t F_e = E$

¹⁴Or *isometric*.

on the matrix of F in any orthonormal basis in V . A matrix $C \in \text{Mat}_n(\mathbb{R})$ is called *orthogonal* if $C^t C = E$, or equivalently, $C^t = C^{-1}$. Thus, a map F is orthogonal if and only if its matrix in some orthonormal basis is orthogonal. The orthogonal matrices form the multiplicative groups

$$\begin{aligned} O_n(\mathbb{R}) &\stackrel{\text{def}}{=} \{C \in \text{Mat}_n(\mathbb{R}) \mid C^t C = E\}, \\ \text{SO}_n(\mathbb{R}) &\stackrel{\text{def}}{=} \{C \in O_n(\mathbb{R}) \mid \det C = 1\}, \end{aligned}$$

called the *orthogonal* and *special orthogonal* real matrix groups.

Example 10.10 (Isometries of the Euclidean Line) Let F be an orthogonal automorphism of the Euclidean line spanned by the vector v . Then $Fv = \lambda v$ and $|v| = |Fv| = |\lambda| \cdot |v|$ forces $\lambda = \pm 1$. Thus, the isometries of the Euclidean line are exhausted by $\pm \text{Id}$.

Example 10.11 (Isometries of the Euclidean Plane) Let an orthogonal automorphism of the Euclidean plane U have matrix

$$F = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in some orthonormal basis e_1, e_2 of U . The orthogonality relation $F^t F = E$ is equivalent to the system of equations

$$\begin{cases} a^2 + c^2 = 1, \\ b^2 + d^2 = 1, \\ ab + cd = 0. \end{cases}$$

All solutions of the first two equations are parametrized as

$$\begin{aligned} a &= \cos \varphi, & c &= \sin \varphi, \\ b &= \sin \psi, & d &= \cos \psi. \end{aligned}$$

Then the third equation is equivalent to the relation $\sin(\psi + \varphi) = 0$. Hence, up to addition of integer multiples of 2π , either $\psi = \varphi$ or $\psi = \pi - \varphi$. In the first case,

$$F = \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}$$

is the counterclockwise rotation through the angle φ about the origin. In the second case,

$$F = \begin{pmatrix} \cos \varphi & \sin \varphi \\ \sin \varphi & -\cos \varphi \end{pmatrix}$$

is the previous rotation composed with the preceding orthogonal reflection $e_1 \mapsto e_1$, $e_2 \mapsto -e_2$ in the first coordinate axis. Such a composition is the reflection in the bisector of the angle between the vectors e_1 and Fe_1 (see Fig. 10.4).

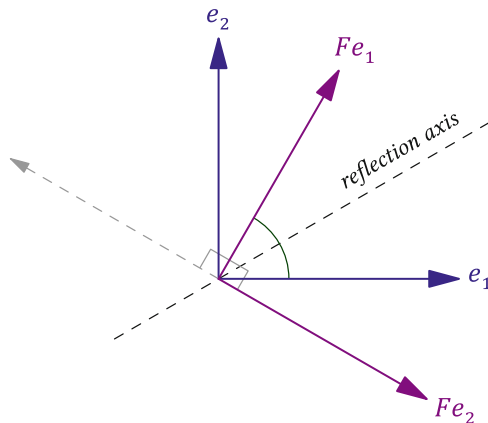


Fig. 10.4 A reflection composed with a rotation is a reflection

Exercise 10.11 Prove this.

Thus, the proper linear orthogonal automorphisms of the Euclidean plane are exhausted by rotations about the origin, while the improper linear orthogonal automorphisms are exhausted by the orthogonal reflections in lines passing through the origin.

Example 10.12 (Reflections in Hyperplanes) A vector $e \in V$ is called a *unit vector* if $|e| = 1$, or equivalently, $(e, e) = 1$. Associated with such a vector is its orthogonal hyperplane $e^\perp \subset V$ and an improper linear isometry $\sigma_e : V \rightarrow V$ that sends e to $-e$ and acts identically on e^\perp (see Fig. 10.5). The isometry σ_e is called an *orthogonal reflection*¹⁵ in the hyperplane e^\perp . In the language of formulas, σ_e is described as

$$\sigma_e : v \mapsto v - 2(v, e)e. \quad (10.27)$$

Exercise 10.12 Verify that the map (10.27) is linear, acts identically on e^\perp , sends e to $-e$, and preserves the inner product.

¹⁵Or just a *reflection* for short.

For an arbitrary nonzero vector $a \in V$, we write σ_a for the orthogonal reflection in the hyperplane a^\perp . It coincides with the reflection σ_e for the unit vector $e = a/|a|$ and is described by the formula

$$\sigma_a(v) = v - 2 \frac{(v, a)}{(a, a)} \cdot a. \quad (10.28)$$

Note that $\sigma_a = \sigma_b$ if and only if a and b are proportional.

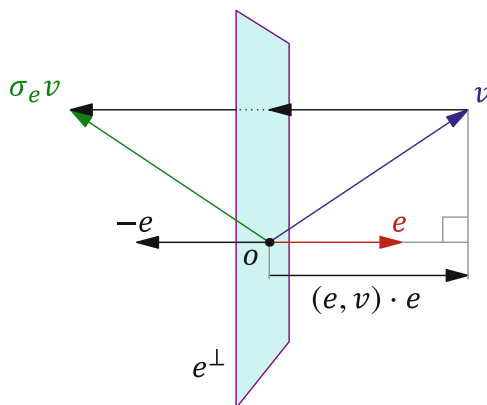


Fig. 10.5 Reflection σ_e

Exercise 10.13 Show that two nonzero vectors of equal lengths can be swapped by appropriate reflection and deduce from this that every linear orthogonal automorphism of V can be split into the composition of at most $\dim V$ reflections in hyperplanes.

If a and b are not proportional, the composition of reflections $\sigma_b \sigma_a$ acts identically on the subspace $a^\perp \cap b^\perp$ of codimension 2 and induces a proper isometry in the orthogonal complementary 2-dimensional plane spanned by a, b . Such an isometry has to be a rotation. Looking how it acts on the basis a, b , we conclude that the line a^\perp is rotated in the direction of the line b^\perp by the doubled acute angle between these lines.

Example 10.13 (Proper Isometries of 3-Dimensional Euclidean Space) By [Exercise 10.13](#), a proper isometry F of 3-dimensional Euclidean space V is either the identity map Id_V or a composition of reflections $F = \sigma_b \sigma_a$ in two different 2-dimensional planes a^\perp and b^\perp . As was explained at the very end of [Example 10.12](#), such a composition is the rotation about the line $a^\perp \cap b^\perp$, which is perpendicular to both vectors a, b , in the direction from the plane a^\perp to the plane b^\perp by the doubled acute angle between them. Thus, each nonidentical proper linear isometry of Euclidean 3-space is a rotation about some line. This fact is known as *Euler's theorem*.

Problems for Independent Solution to Chap. 10

Problem 10.1 In the standard Euclidean structure on a real coordinate space construct an explicit orthonormal basis for (a) the hyperplane $x_1 + x_2 + \cdots + x_n = 0$ in \mathbb{R}^n , (b) the subspace in \mathbb{R}^4 spanned by the vectors $(1, 2, 2, -1)$, $(1, 1, -5, 3)$, $(3, 2, 8, -7)$, (c) the orthogonal complement to the previous subspace.

Problem 10.2 Let $U \subset \mathbb{R}^4$ be the solution space of the system of linear equations

$$\begin{cases} 2x_1 + x_2 + 3x_3 - x_4 = 0, \\ 3x_1 + 2x_2 - 2x_4 = 0, \\ 3x_1 + x_2 + 9x_3 - x_4 = 0. \end{cases}$$

Write down a system of linear equations whose solution space is U^\perp .

Problem 10.3 For given $a \in \mathbb{R}^n$ and $d_1, d_2 \in \mathbb{R}$, find the distance between the parallel hyperplanes $(a, x) = d_1$ and $(a, x) = d_2$ in \mathbb{R}^n .

Problem 10.4 Given $k + 1$ distinct points $p_0, p_1, \dots, p_k \in \mathbb{R}^n$ that do not lie in a common $(k - 1)$ -dimensional affine subspace, describe the locus of all points equidistant from all the p_i .

Problem 10.5 Find the maximal number of distinct nonzero vectors in \mathbb{R}^n such that all the angles between them are obtuse.¹⁶

Problem 10.6 (Sphere) For given point $c \in \mathbb{R}^n$ and positive number $r \in \mathbb{R}$, the geometric figure


$$S_{c,r}^{n-1} \stackrel{\text{def}}{=} \{x \in \mathbb{R}^n : |c, x| = r\}$$

is called the $(n - 1)$ -sphere of radius r with center c . Show that every set of $n + 1$ points in \mathbb{R}^n lie either on a hyperplane or on a unique $(n - 1)$ -sphere.

Problem 10.7 (Cube) The figure $I^n \stackrel{\text{def}}{=} \{(x_1, x_2, \dots, x_n) \in \mathbb{R}^n \mid \forall i \ |x_i| \leq 1\}$ is called a *standard n -cube*.

- Draw a plane projection of I^4 in which all the vertices of I^4 are distinct.
- Describe a three-dimensional involute of the boundary¹⁷ of I^4 and explain how its 2-dimensional faces should be glued together in order to get the actual 3-dimensional boundary of I^4 .
- For all $0 \leq k \leq (n - 1)$, find the total number of k -dimensional faces of I^n .
- A segment $[v, -v]$ joining two opposite vertices of I^n is called an *internal diagonal*. How many internal diagonals are there in I^n ?

¹⁶In \mathbb{R}^2 , for example, there are at most three such vectors; in \mathbb{R}^3 , there are at most four.

¹⁷Such an involute consists of 3-dimensional cubes in \mathbb{R}^3 glued somehow along their 2-dimensional faces like the flat involute  of the 2-dimensional surface of the brick I^3 .

- (e) How many internal diagonals of I^n are perpendicular to a given internal diagonal?
- (f) Calculate the length of an internal diagonal¹⁸ in I^n and its limit as $n \rightarrow \infty$.
- (g) Calculate the lengths of segments between the orthogonal projections of vertices onto an internal diagonal.
- (h) Calculate the angle between an internal diagonal and an edge of I^n . Find its limit as $n \rightarrow \infty$.
- (i) Calculate the angle between an internal diagonal and a face¹⁹ of I^n . Find its limit as $n \rightarrow \infty$.
- (j) How many mirror hyperplanes²⁰ does I^n have?

Problem 10.8 Give an explicit description of each 3-dimensional polyhedron cut out of I^4 by the 3-dimensional hyperplane $x_1 + x_2 + x_3 + x_4 = c$ as c runs through $[-4, 4]$.

Problem 10.9 (Simplex) The convex hull²¹ of the heads of the standard basis vectors in \mathbb{R}^{n+1} ,

$$\Delta^n \stackrel{\text{def}}{=} \{(x_0, x_1, \dots, x_n) \in \mathbb{R}^{n+1} \mid \text{all } x_i \geq 0 \text{ and } \sum x_i = 1\},$$

is called the *standard n -simplex*. Draw Δ^1 and Δ^2 in the plane. Then:

- (a) Draw some plane projections of Δ^3 and Δ^4 on which all the vertices are distinct.
- (b) Describe some three-dimensional involute of the boundary of Δ^4 and explain how its 2-dimensional faces should be glued to get the actual 3-dimensional boundary of Δ^4 .
- (c) For all $0 \leq k \leq (n-1)$, find the total number of k -dimensional faces of Δ^n .
- (d) Show that there is a unique $(n-1)$ -sphere touching all faces of Δ^n . Find the radius of this sphere and its limit as $n \rightarrow \infty$.
- (e) Show that there is a unique $(n-1)$ -sphere containing all vertices of Δ^n . Find the radius of this sphere and its limit as $n \rightarrow \infty$.
- (f) Find the length of the perpendicular drawn from a vertex of Δ^n onto the opposite face and compute its limit as $n \rightarrow \infty$.
- (g) Find the angle between an edge of Δ^n and one of the two faces that does not contain this edge; calculate the limit of this angle as $n \rightarrow \infty$.
- (h) For each $1 \leq m \leq (n-1)$, find the distance between nonintersecting m - and $(n-m-1)$ -dimensional faces of Δ^n .

¹⁸That is, the diameter of the sphere circumscribed about I^n .

¹⁹That is, an $(n-1)$ -dimensional face.

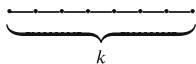
²⁰That is, hyperplanes $e^\perp \subset \mathbb{R}^n$ such that the reflection $\sigma_e : \mathbb{R}^n \rightarrow \mathbb{R}^n$ sends I^n to itself (see Example 10.12 on p. 246 for details on reflections).

²¹See Example 6.16 on p. 145.

Problem 10.10 Consider the standard 4-simplex $ABCDE$ and write X for the midpoint of the segment joining the centers of the 2-dimensional faces ABC and CDE . Show that there is a unique line YZ passing through X and intersecting both the line AE and the plane BCD at some points Y and Z respectively. Find $\overrightarrow{XY} : \overrightarrow{YZ}$, that is, $\lambda \in \mathbb{R}$ such that $\overrightarrow{XY} = \lambda \cdot \overrightarrow{YZ}$.

Problem 10.11 Give an explicit description of each 3-dimensional polyhedron cut out of $\Delta^4 \subset \mathbb{R}^5$ by the hyperplane (a) $x_1 = \text{const}$, (b) $x_1 + x_2 = \text{const}$.

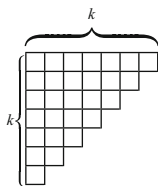
Problem 10.12 (Volume of a Simplex) A 1-dimensional echelon pyramid of height k consists of $\Pi_k^1 \stackrel{\text{def}}{=} k$ unit segments aligned along the horizontal coordinate axis:



A 2-dimensional echelon pyramid of height k consists of

$$\Pi_k^2 \stackrel{\text{def}}{=} \Pi_k^1 + \Pi_{k-1}^1 + \cdots + \Pi_1^1$$

unit squares aligned along the vertical axis:



Similarly, an n -dimensional echelon pyramid of height k consists of

$$\Pi_k^n = \Pi_k^{n-1} + \Pi_{k-1}^{n-1} + \cdots + \Pi_1^{n-1}$$

unit $(n-1)$ -cubic bricks stacked in piles along the n th coordinate axis. Calculate the total number of these bricks. Send k to infinity and find the ratio between the Euclidean volume of an n -dimensional cube and the Euclidean volume of the n -dimensional simplex obtained as the convex hull of some vertex v of the cube and all vertices joined with v by an edge of the cube.

Problem 10.13 (Cocube) The convex hull of the centers of the faces of the standard cube $I^n \subset \mathbb{R}^n$ is called the *standard n -dimensional cocube* and is denoted by C^n .

- (a) Describe C^n by an explicit system of linear inequalities.
- (b) For all $0 \leq k \leq (n-1)$, find the total number of k -dimensional faces of C^n .
- (c) Find the length of an edge of C^n and its limit as $n \rightarrow \infty$.
- (d) Find the radius of the $(n-1)$ -sphere inscribed in C^n and its limit as $n \rightarrow \infty$.

Problem 10.14 For k points p_1, p_2, \dots, p_k in affine Euclidean space write D_{p_1, p_2, \dots, p_k} for the $k \times k$ matrix with elements $d_{ij} = |p_i, p_j|^2$, and C_{p_1, p_2, \dots, p_k} for the $(k+1) \times (k+1)$ matrix whose elements c_{ij} are numbered by $0 \leq i, j \leq k$ and are equal to d_{ij} for $1 \leq i, j \leq k$, whereas $c_{00} = 0$ and $c_{0j} = c_{i0} = 1$ for all $1 \leq i, j \leq k$. As usual, G_{w_1, w_2, \dots, w_m} denotes the Gram matrix of vectors w_1, w_2, \dots, w_m . Prove that:

- (a) $2^n \det G_{\overrightarrow{p_0 p_1}, \overrightarrow{p_0 p_2}, \dots, \overrightarrow{p_0 p_n}} = (-1)^{n+1} \det C_{p_0, p_1, \dots, p_n}$ (note that the matrices have different sizes).
- (b) $n+1$ points $p_0, p_1, \dots, p_n \in \mathbb{R}^n$ lie in a hyperplane if and only if $\det C_{p_0, p_1, \dots, p_n} = 0$.
- (c) $n+2$ points $p_0, p_1, \dots, p_{n+1} \in \mathbb{R}^n$ lie either in a hyperplane or on a sphere if and only if $\det D_{p_0, p_1, \dots, p_{n+1}} = 0$.
- (d) The radius r of the sphere circumscribed about the n -simplex $p_0 p_1 \dots p_n$ satisfies the equality $2r^2 = -\det D_{p_0, p_1, \dots, p_n} / \det C_{p_0, p_1, \dots, p_n}$.

Problem 10.15 (Orthogonal Polynomials) Check that the following inner products provide $\mathbb{R}[x]$ with a Euclidean structure:

$$\begin{aligned} \text{(a)} \quad (f, g) &= \int_{-1}^1 f(x)g(x) (1-x^2)^{-1/2} dx, & \text{(b)} \quad (f, g) &= \int_0^{+\infty} f(x)g(x)e^{-x} dx, \\ \text{(c)} \quad (f, g) &= \int_{-\infty}^{+\infty} f(x)g(x)e^{-x^2} dx, & \text{(d)} \quad (f, g) &= \int_{-1}^1 f(x)g(x) dx. \end{aligned}$$

Consider a sequence of

- (1) Chebyshev polynomials $T_n(x) = \cos(n \arccos x)$,
- (2) Laguerre polynomials $L_n(x) = e^x \frac{d^n}{dx^n} (e^{-x} x^n)$,
- (3) Hermite polynomials $E_n(x) = e^{x^2} \frac{d^n}{dx^n} e^{-x^2}$,
- (4) Legendre polynomials $P_n(x) = \frac{d^n}{dx^n} (1-x^2)^n$.

For each sequence, indicate the Euclidean structure in which this sequence is orthogonal and compare the sequence with the output of Gram-Schmidt orthogonalization applied to the standard monomial basis x^k in $\mathbb{R}[x]$.

Problem 10.16* Find the minimum of $\int_{-1}^1 f^2(x) dx$ over all degree- k monic polynomials $f \in \mathbb{R}[x]$. To begin with, consider $k = 2, 3, 4$.

Problem 10.17 In the space of continuous functions $[-\pi, \pi] \rightarrow \mathbb{R}$ with inner product

$$(f, g) = \int_{-\pi}^{\pi} f(x)g(x) dx,$$

find the polynomial of degree at most 3 closest to $\sin x$.

Problem 10.18 Check that the inner product $(A, B) = \text{tr}(AB^t)$ provides $\text{Mat}_n(\mathbb{R})$ with a Euclidean structure. Describe the orthogonal complements to (a) upper triangular matrices,²² (b) symmetric matrices,²³ (c) skew-symmetric matrices,²⁴ (d) traceless matrices.²⁵

Problem 10.19 (Adjoint Linear Maps) Show that for every linear map of Euclidean vector spaces $F : U \rightarrow W$ there exists a unique linear map²⁶ $F^\vee : W \rightarrow U$ such that $(F^\vee w, u) = (w, Fu)$ for all $w \in W$ and $u \in U$. Check that $(F_1 \circ F_2)^\vee = F_2^\vee \circ F_1^\vee$, $\ker F^\vee = (\text{im } F)^\perp$, $\text{im } F^\vee = (\ker F)^\perp$. For bases $\mathbf{u} = (u_1, u_2, \dots, u_n)$, $\mathbf{w} = (w_1, w_2, \dots, w_m)$ of U, W , prove that the matrix $F_{\mathbf{u}\mathbf{w}}^\vee$ of F^\vee is expressed in terms of the matrix $F_{\mathbf{w}\mathbf{u}}$ of F and Gramians $G_{\mathbf{u}}, G_{\mathbf{w}}$ as $F_{\mathbf{u}\mathbf{w}}^\vee = G_{\mathbf{u}}^{-1} F_{\mathbf{w}\mathbf{u}}^t G_{\mathbf{w}}$.

Problem 10.20 (Normal Linear Endomorphisms) Show that for every Euclidean vector space V , the following properties of a linear endomorphism $F : V \rightarrow V$ are equivalent²⁷:

- (a) $F^\vee \circ F = F \circ F^\vee$,
- (b) $\forall v \in V |F^\vee v| = |Fv|$,
- (c) $\forall u, w \in V (F^\vee u, F^\vee w) = (Fu, Fw)$.

²²A matrix $C = (c_{ij})$ is called *upper triangular* if $c_{ij} = 0$ for all $i > j$.

²³A matrix $C = (c_{ij})$ is called *symmetric* if $c_{ij} = c_{ji}$ for all i, j .

²⁴A matrix $C = (c_{ij})$ is called *skew-symmetric*, if $c_{ij} = -c_{ji}$ for all i, j .

²⁵A matrix $C = (c_{ij})$ is called *traceless* if $\text{tr} C \stackrel{\text{def}}{=} \sum_i c_{ii} = 0$.

²⁶It is called the *Euclidean adjoint* to F .

²⁷A linear endomorphism F possessing these properties is called *normal*.

Chapter 11

Projective Spaces

11.1 Projectivization

11.1.1 Points and Charts

Let V be a vector space of dimension $(n + 1)$ over a field \mathbb{k} . Besides the $(n + 1)$ -dimensional affine space¹ $\mathbb{A}^{n+1} = \mathbb{A}(V)$, associated with V is the n -dimensional *projective space* $\mathbb{P}_n = \mathbb{P}(V)$, called the *projectivization* of V . By definition, points of $\mathbb{P}(V)$ are 1-dimensional vector subspaces in V , or equivalently, lines in $\mathbb{A}(V)$ passing through the origin. To observe such points as usual “dots,” we have to use a screen, that is, an n -dimensional affine hyperplane in $\mathbb{A}(V)$ that does not pass through the origin (see Fig. 11.1).

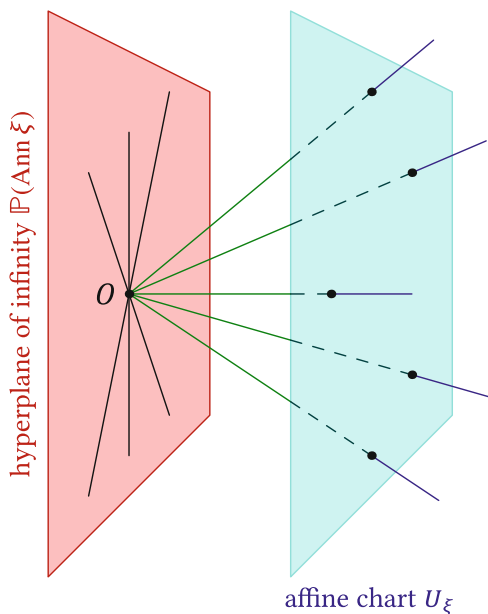
Every affine hyperplane of this sort is described by an inhomogeneous linear equation $\xi(x) = 1$, where $\xi \in V^*$ is a nonzero linear form on V . We write $U_\xi = \{v \in V \mid \langle v, \xi \rangle = 1\}$ for such a screen and call it the *affine chart* provided by the covector ξ .

Exercise 11.1 Make certain for yourself that the rule $\xi \mapsto U_\xi$ establishes a bijection between nonzero covectors $\xi \in V^*$ and affine hyperplanes in $\mathbb{A}(V)$ that do not pass through the origin.

Not all points of $\mathbb{P}(V)$ are visible in a chart U_ξ . The complement $\mathbb{P}(V) \setminus U_\xi$ consists of 1-dimensional subspaces spanned by nonzero vectors $v \in V$ parallel to U_ξ , i.e., lying inside the n -dimensional vector subspace $\text{Ann}(\xi) = \{v \in V \mid \langle v, \xi \rangle = 0\}$ in V . They form an $(n - 1)$ -projective space $\mathbb{P}_{n-1} = \mathbb{P}(\text{Ann}(\xi))$, called the *hyperplane at infinity*² of the chart U_ξ . The points of $\mathbb{P}(\text{Ann}(\xi))$ can be thought of as *directions* in the affine space U_ξ . Thus, as a set, projective space splits into the disjoint union

¹See Sect. 6.5 on p. 142.

²Or just the *infinity*.

Fig. 11.1 Projective space

$\mathbb{P}_n = \mathbb{A}^n \sqcup \mathbb{P}_{n-1}$. Repeating this procedure, we obtain the decomposition $\mathbb{P}_n = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \dots \sqcup \mathbb{A}^0$, where the last element $\mathbb{A}^0 = \mathbb{P}_0$ is one point.

Exercise 11.2 Over the finite field of q elements, compute independently the cardinalities of \mathbb{P}_n and $\mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \dots \sqcup \mathbb{A}^0$. What kind of identity involving q do you get?

11.1.2 Global Homogeneous Coordinates

Let us fix a basis x_0, x_1, \dots, x_n in V^* and identify V with the coordinate space \mathbb{K}^{n+1} by the rule $v \mapsto (x_0(v), x_1(v), \dots, x_n(v))$. Two nonzero vectors $v = (x_0, x_1, \dots, x_n)$ and $w = (y_0, y_1, \dots, y_n)$ produce the same point $p \in \mathbb{P}_n$ if and only if their coordinates are proportional, i.e., $x_\mu : x_\nu = y_\mu : y_\nu$ for all $0 \leq \mu \neq \nu \leq n$, where the equalities $0 : x = 0 : y$ and $x : 0 = y : 0$ are allowed as well. Thus, the collection of ratios $(x_0 : x_1 : \dots : x_n)$ matches some point $p \in \mathbb{P}_n$. This collection is called the *homogeneous coordinates* of p in the basis x_0, x_1, \dots, x_n of V^* .

11.1.3 Local Affine Coordinates

Let us fix an affine chart $U_\xi = \{x \in \mathbb{A}(V) \mid \xi(x) = 1\}$ provided by the covector $\xi \in V^*$. Choose n linear forms $\xi_1, \xi_2, \dots, \xi_n \in V^*$ such that $\xi, \xi_1, \xi_2, \dots, \xi_n$ form a basis in V^* , and write $e_0, e_1, \dots, e_m \in V$ for the dual basis in V . Then e_0, e_1, \dots, e_m form an affine coordinate system³ in $U_\xi \subset \mathbb{A}(V)$ with the origin at $e_0 \in U_\xi$ and the basis e_1, e_2, \dots, e_m in the vector space $\text{Ann}(\xi) \subset V$ with which the affine space U_ξ is associated. The coordinates of the points in this system are called *local affine coordinates* in U_ξ . Note that they are well defined only within U_ξ . The local affine coordinates of a point $p \in \mathbb{P}_n = \mathbb{P}(V)$ with homogeneous coordinates $(x_0 : x_1 : \dots : x_n)$ are evaluated as follows. Among all proportional vectors representing p we pick the vector $v = p/\xi(p)$ that has $\xi(v) = 1$ and therefore lies in U_ξ . Note that the equality $\xi(p) = 0$ means that $p \notin U_\xi$. Then we evaluate the linear forms $\xi_1, \xi_2, \dots, \xi_n$ on this vector. Note that the resulting affine coordinates

$$\xi_i(v) = \xi_i(p)/\xi(p), 1 \leq i \leq n,$$

are not linear but linear fractional functions of the homogeneous coordinates. In particular, as p runs to infinity, that is, $\xi(p) \rightarrow 0$, the local affine coordinates of p actually tend to infinite values.

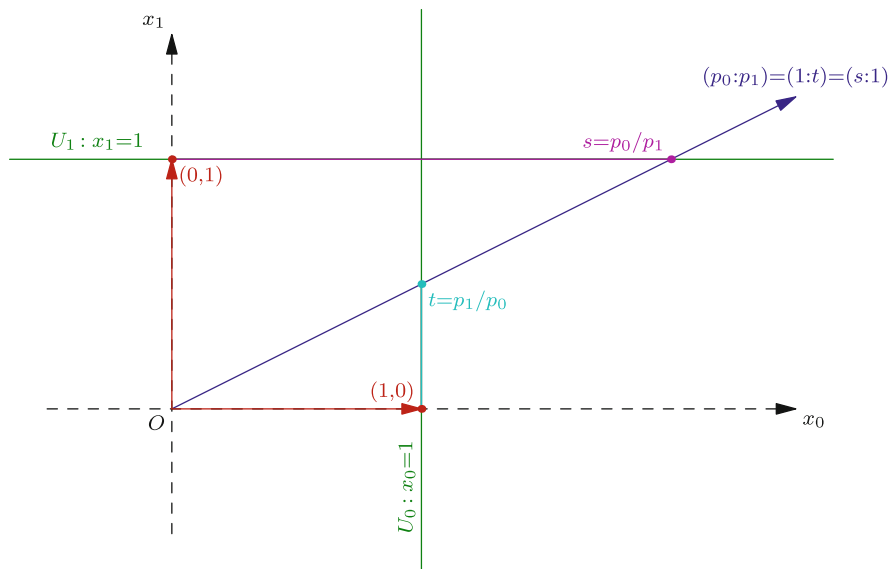


Fig. 11.2 Standard affine charts on \mathbb{P}_1

³See Sect. 6.5.2 on p. 143.

Example 11.1 (The Projective Line) The projective line $\mathbb{P}_1 = \mathbb{P}(\mathbb{k}^2)$ is covered by two affine charts $U_0 = U_{x_0}$, $U_1 = U_{x_1}$, that is, by two affine lines defined by the equations $x_0 = 1$ and $x_1 = 1$ (see Fig. 11.2). The chart U_0 contains all points except for one point $(0 : 1)$ represented by the vertical coordinate axis. This is the only infinite point for the chart U_0 . Every other point $(x_0 : x_1)$ with $x_0 \neq 0$ is visible in U_1 as $(1 : x_1/x_0)$. The function $t = x_1|_{U_0} = x_1/x_0$ can be used as a local affine coordinate within U_0 . The chart U_1 consists of points $(x_0 : x_1) = (x_0/x_1 : 1)$ with $x_1 \neq 0$, and the function $s = x_0|_{U_1} = x_0/x_1$ can be used as a local affine coordinate within U_1 . The only infinite point for U_1 is $(1 : 0)$, represented by the horizontal coordinate axis. Local affine coordinates s, t of the same point $(x_0 : x_1) \in \mathbb{P}_1$ lying within $U_0 \cap U_1$ are related by $s = 1/t$. Thus, \mathbb{P}_1 consists of two copies of the affine line \mathbb{A}^1 (one line with coordinate s , another with coordinate t) glued together along the complements to their origins by the following rule: point s on the first line is glued with point $t = 1/s$ on the second.

For $\mathbb{k} = \mathbb{R}$, the result of such gluing can be identified with a circle of diameter 1 glued from two diametrically opposite tangent lines mapped onto the circle via central projections from the opposite points of tangency (see Fig. 11.3). Similarly, for $\mathbb{k} = \mathbb{C}$, two copies of copies of $\mathbb{A}^1 = \mathbb{C}$ glued together by the rule $s \leftrightarrow 1/s$ produce a sphere of diameter 1 consisting of two tangent planes drawn through the south and north poles and mapped onto the sphere by the central projections from opposite poles (see Fig. 11.4). Indeed, if the orientations of the planes are chosen⁴ as in Fig. 11.4, then the complex numbers s, t corresponding to the same point of the sphere have opposite arguments, and their moduli are inverses of each other by Fig. 11.3.

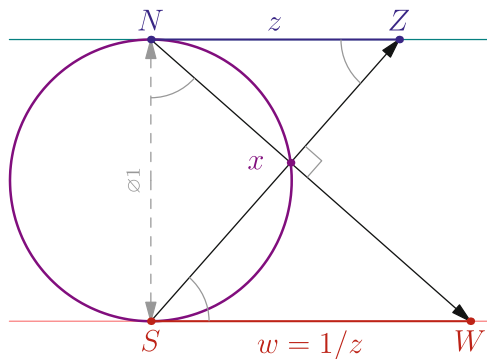


Fig. 11.3 $\mathbb{P}_1(\mathbb{R}) \simeq S^1$

⁴These orientations will coincide when we overlap the planes by a continuous movement along the surface of the sphere.

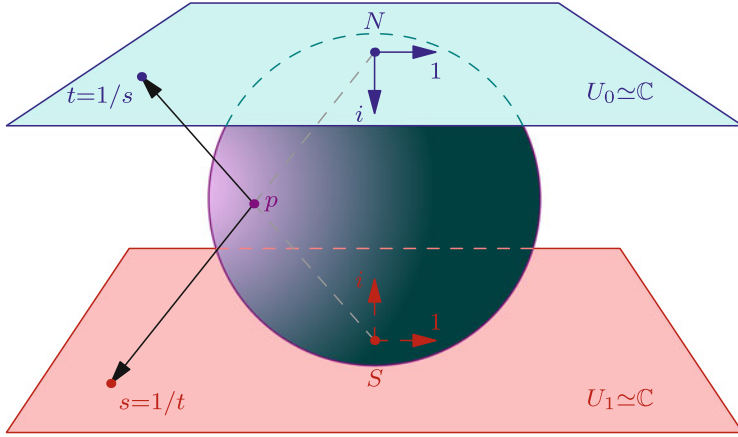


Fig. 11.4 $\mathbb{P}_1(\mathbb{C}) \simeq S^2$

Example 11.2 (Standard Affine Atlas on \mathbb{P}_n) For $\mathbb{P}_n = \mathbb{P}(\mathbb{K}^{n+1})$, the collection of $(n+1)$ affine charts $U_\nu = U_{x_\nu}$, $0 \leq \nu \leq n$, i.e., hyperplanes $x_\nu = 1$ in \mathbb{A}^{n+1} , is called the *standard affine atlas* on \mathbb{P}_n . For each ν , the point $e_\nu \in U_\nu$ is taken as the origin of the standard affine coordinate system in U_ν , and the functions

$$t_i^{(\nu)} \stackrel{\text{def}}{=} x_i|_{U_\nu} = \frac{x_i}{x_\nu} \quad \text{for } 0 \leq i \leq n, i \neq \nu,$$

are used as the standard affine coordinates. The intersection $U_\mu \cap U_\nu$ consists of all x with both homogeneous coordinates x_μ, x_ν nonzero. In the standard affine coordinates in U_μ (respectively in U_ν), the locus of such points is described by the inequality $t_\nu^{(\mu)} \neq 0$ (respectively by the inequality $t_\mu^{(\nu)} \neq 0$). The affine coordinates of the points $t^{(\mu)} \in U_\mu$ and $t^{(\nu)} \in U_\nu$ representing the same point in \mathbb{P}_n are related by

$$t_\nu^{(\mu)} = 1/t_\mu^{(\nu)} \quad \text{and} \quad t_i^{(\mu)} = t_i^{(\nu)} / t_\mu^{(\nu)} \quad \text{for } i \neq \mu, \nu. \quad (11.1)$$

The right-hand sides of these equalities are called *transition functions* from the local coordinates $t^{(\nu)}$ in U_ν to the local coordinates $t^{(\mu)}$ in U_μ . Therefore, \mathbb{P}_n is glued from $(n+1)$ disjoint copies U_0, U_1, \dots, U_n of the affine space \mathbb{A}^n by the gluing rules (11.1).

11.2 Polynomials Revisited

11.2.1 Polynomial Functions on a Vector Space

Every choice of basis x_0, x_1, \dots, x_n in the vector space V^* dual to an $(n + 1)$ -dimensional vector space V allows us to treat each polynomial $f \in \mathbb{k}[x_0, x_1, \dots, x_n]$ as a *polynomial function* $\tilde{f} : V \rightarrow \mathbb{k}$ that takes a vector $v \in V$ with coordinates $v_i = x_i(v) \in \mathbb{k}$ to the result of the evaluation $\text{ev}_{(v_0, v_1, \dots, v_n)}(f) = f(v_0, v_1, \dots, v_n) \in \mathbb{k}$. Thus, we get a homomorphism of \mathbb{k} -algebras

$$\alpha : \mathbb{k}[x_1, x_2, \dots, x_n] \rightarrow \mathbb{k}^V, \quad f \mapsto \tilde{f}, \quad (11.2)$$

which maps the polynomial algebra to the algebra of functions $V \rightarrow \mathbb{k}$. Its image is called the *algebra of polynomial functions* on V .

Exercise 11.3 Check that the \mathbb{k} -subalgebra $\text{im } \alpha \subset \mathbb{k}^V$ does not depend on the choice of basis in V^* .

Proposition 11.1 *For an infinite ground field \mathbb{k} , the homomorphism (11.2) is injective. If \mathbb{k} is finite and $\dim V < \infty$, then the homomorphism (11.2) is surjective and has nonzero kernel.*

Proof The first statement was already established in [Exercise 9.6](#) on p. 213. For $\mathbb{k} = \mathbb{F}_q$ and $V = \mathbb{F}_q^n$, the functions $V \rightarrow \mathbb{k}$ form a vector space of dimension q^n with a basis formed by δ -functions δ_p , $p \in \mathbb{k}^n$, such that $\delta(p) = 1$ and $\delta_p(q) = 0$ for all $q \neq p$.

Exercise 11.4 Verify that $\delta_p = \tilde{f}$ for

$$f(x_1, \dots, x_n) = \frac{\prod_i \prod_{\xi \neq p_i} (x_i - \xi)}{\prod_i \prod_{\xi \neq p_i} (p_i - \xi)},$$

where ξ runs through $\mathbb{F}_q \setminus p_i$ in both products.

Therefore, the homomorphism (11.2) is surjective. Since $\mathbb{k}[x_1, x_2, \dots, x_n]$ is infinite-dimensional as a vector space over \mathbb{k} , the homomorphism (11.2) has nonzero kernel. \square

11.2.2 Symmetric Algebra of a Vector Space

It follows from Proposition 11.1 and [Exercise 11.3](#) that for an infinite field \mathbb{k} , the polynomial algebra $\mathbb{k}[x_0, x_1, \dots, x_n]$ is isomorphic to the algebra of polynomial functions $V \rightarrow \mathbb{k}$, and the latter does not depend on the choice of variables x_i forming a basis of V^* . This suggests that the polynomial algebra should have some

coordinate-free description in intrinsic terms of V^* . Such a description is given below.

The space of linear homogeneous polynomials in x_0, x_1, \dots, x_n coincides with V^* . Every homogeneous polynomial $f(x_0, x_1, \dots, x_n)$ of higher degree d can be written (in many ways) as a finite sum of products $a_1 \cdot a_2 \cdots a_d$, where all a_v belong to V^* . Such products are called *commutative monomials* of degree d in the covectors $a_i \in V^*$. They certainly are linearly related, because for all $a, b \in V^*$, all $\lambda, \mu \in \mathbb{k}$, and all monomials m', m'' of total degree $d - 1$, the *distributive* and *commutative* laws

$$\begin{aligned} m'(\lambda \cdot a + \mu \cdot b)m'' - \lambda \cdot m'am''m' - \mu \cdot m'bm'' &= 0, \\ m'abm'' - m'bam'' &= 0, \end{aligned} \quad (11.3)$$

hold. Let us write \mathcal{V}_d^* for the huge⁵ vector space whose basis over \mathbb{k} consists of all words $a_1a_2 \dots a_d$ formed by arbitrary d -tuples of elements $a_v \in V^*$. Thus, the vectors of \mathcal{V}_n^* are formal finite linear combinations of words $a_1a_2 \dots a_d$ with coefficients in \mathbb{k} , and all such words are linearly independent. Write $\mathcal{S}_d^* \subset \mathcal{V}_d^*$ for the linear span of all differences from the left-hand sides of the relations (11.3). The quotient space $S^d V^* \triangleq \mathcal{V}_d^* / \mathcal{S}_d^*$ is called the *n th symmetric power* of the vector space V^* . We put $S^0 V^* \triangleq \mathbb{k}$ and $S^1 V^* \triangleq V^*$. The direct sum

$$SV^* \triangleq \bigoplus_{d \geq 0} S^d V^* \quad (11.4)$$

is called the *symmetric algebra* of the vector space V^* . The multiplication in this algebra maps

$$S^m V^* \times S^d V^* \rightarrow S^{m+d} V^*$$

and is defined as follows. Fix a basis word $w \in \mathcal{V}_m^*$ and define a linear map $L_w : \mathcal{V}_d^* \rightarrow \mathcal{V}_{d+m}^*$ by $m \mapsto wm$ for every basic word $m \in \mathcal{V}_d^*$. It sends differences from the left-hand sides of (11.3) to the same differences but with wm' instead of m' . Hence, L_w sends $\mathcal{S}_d^* \subset \mathcal{V}_d^*$ into $\mathcal{S}_{d+m}^* \subset \mathcal{V}_{d+m}^*$ and therefore produces a well-defined map of quotients $\bar{L}_w : S^d V^* \rightarrow S^{d+m} V^*$. For a finite linear combination of words $f = \sum \lambda_w w$, we put $L_f = \sum \lambda_w L_w$ and $\bar{L}_f = \sum \lambda_w \bar{L}_w$.

Exercise 11.5 Check that $\bar{L}_f = 0$ for every $f \in \mathcal{S}_d^*$.

⁵It is infinite dimensional as soon V is infinite as a set.

Thus, \bar{L}_f depends only on the class of f in the quotient space $S^m V^*$. Therefore, the assignment $f, g \mapsto \bar{L}_f(g)$ produces a well-defined *multiplication map*

$$S^m V^* \times S^d V^* \rightarrow S^{m+d} V^*$$

that is linear in the both arguments f, g . Since commutative monomials are multiplied by concatenation,

$$b_1 b_2 \dots b_m \cdot a_1 a_2 \dots a_d = b_1 b_2 \dots b_m a_1 a_2 \dots a_d,$$

the algebra SV^* is associative. The second equality in (11.3), which holds in the quotient space $S^{m+d} V^*$, says that the algebra SV^* is commutative. Taking a bit of liberty, we call elements of SV^* *polynomials* on V , and the elements of $S^d V^* \subset SV^*$ will be called *homogeneous polynomials* of degree d . Such terminology is partially justified by the next claim.

Proposition 11.2 *If the covectors x_0, x_1, \dots, x_n form a basis of V^* , then the commutative monomials $x_0^{m_0} x_1^{m_1} \dots x_n^{m_n}$ formed from them constitute a basis in SV^* .*

Proof By definition, a monomial $x_0^{m_0} x_1^{m_1} \dots x_n^{m_n}$ is a product of m_0 basic covectors x_0 , m_1 basic covectors x_1 , \dots , m_n basic covectors x_n . Since SV^* is commutative, this monomial is completely determined by the sequence of nonnegative integers m_0, m_1, \dots, m_n . Let us show that the monomials $x_0^{m_0} x_1^{m_1} \dots x_n^{m_n}$ with $\sum m_i = d$ form a basis in $S^d V^*$. They certainly span $S^d V^*$, because the relations (11.3) allow every product $a_1 a_2 \dots a_d$ to be expanded as a linear combination of monomials compounded from the x_i . To prove their linear independence, it is enough to construct a linear form $S^d V^* \rightarrow \mathbb{k}$ that equals 1 on an arbitrarily prescribed monomial $x_0^{m_0} x_1^{m_1} \dots x_n^{m_n}$ and vanishes on all other monomials. By Proposition 7.4 on p. 163, a linear form on the quotient space $S^d V^* = \mathcal{V}_d^* / \mathcal{S}_d^*$ is the same as a linear form $\varphi : \mathcal{V}_d^* \rightarrow \mathbb{k}$ annihilating \mathcal{S}_d^* . By Lemma 7.1 on p. 155, every linear form $\varphi : \mathcal{V}_d^* \rightarrow \mathbb{k}$ is the same as a function on the basis of \mathcal{V}_d^* formed by words $a_1 a_2 \dots a_d$. The latter is nothing but an arbitrary map

$$\widetilde{\varphi} : \underbrace{V^* \times V^* \times \dots \times V^*}_d \rightarrow \mathbb{k} \quad (a_1, a_2, \dots, a_d) \mapsto \varphi(a_1 a_2 \dots a_d). \quad (11.5)$$

A linear form $\varphi : \mathcal{V}_d^* \rightarrow \mathbb{k}$ annihilates \mathcal{S}_d^* if and only if it vanishes on the left-hand sides of the relations (11.3). In terms of the map (11.5) corresponding to φ , this means that for all $a, b \in V^*$ and all $\lambda, \mu \in \mathbb{k}$, the relations⁶

$$\begin{aligned} \widetilde{\varphi}(\dots, \lambda a + \mu b, \dots) &= \lambda \widetilde{\varphi}(\dots, a, \dots) + \mu \widetilde{\varphi}(\dots, b, \dots), \\ \widetilde{\varphi}(\dots, a, b, \dots) &= \widetilde{\varphi}(\dots, b, a, \dots), \end{aligned} \quad (11.6)$$

⁶Dotted things in (11.6) are not changed.

hold, i.e., that the map (11.5) is *multilinear* and *symmetric*. The first means that $\widetilde{\varphi}$ is uniquely determined by its values on all collections of basis vectors, that is, by the set of numbers

$$\varphi_{i_1, i_2, \dots, i_d} \stackrel{\text{def}}{=} \widetilde{\varphi}(x_{i_1}, x_{i_2}, \dots, x_{i_d}).$$

The multilinear map (11.5) corresponding to such a set takes a d -tuple of vectors $a_v = \sum_{i=0}^n \alpha_{vi} x_i$, where $1 \leq v \leq d$, to the number

$$\widetilde{\varphi}(a_1, a_2, \dots, a_d) = \sum_{i_1, i_2, \dots, i_d} \alpha_{1i_1} \alpha_{2i_2} \cdots \alpha_{di_d} \cdot \varphi_{i_1, i_2, \dots, i_d} \in \mathbb{k} \quad (11.7)$$

(all summation indices i_v vary independently in the range $0 \leq i_v \leq n$).

Exercise 11.6 Check that the map (11.7) is multilinear.

The symmetry property of $\widetilde{\varphi}$ means that the number $\varphi_{i_1, i_2, \dots, i_d} \in \mathbb{k}$ remains fixed under permutations of indices i_1, i_2, \dots, i_d , that is, it depends only on the number m_0 of indices 0, the number m_1 of indices 1, \dots , the number m_n of indices n represented in i_1, i_2, \dots, i_d . Write

$$\widetilde{\varepsilon}_{m_0 m_1 \dots m_n} : V^* \times V^* \times \cdots \times V^* \rightarrow \mathbb{k}$$

for the symmetric multilinear map that equals 1 on all collections of m_0 basis vectors x_0 , m_1 basis vectors x_1, \dots , m_n basis vectors x_n , and vanishes on all the other collections of basis vectors. Its associated linear form $\varepsilon_{m_0 m_1 \dots m_n} : \mathcal{V}_d^* \rightarrow \mathbb{k}$ equals 1 on all words $x_{i_1} x_{i_2} \cdots x_{i_d}$ written by m_0 letters x_0 , m_1 letters x_1, \dots , m_n letters x_n , and vanishes on all the other words compounded from the x_v . The induced linear form on $S^d V^* = \mathcal{V}_d^* / \mathcal{S}_d^*$ sends the monomial $x_0^{k_0} x_1^{k_1} \cdots x_n^{k_n}$ to 1 and annihilates all the other monomials, as required. \square

Corollary 11.1 (From the Proof of Proposition 11.2) *The space of symmetric multilinear maps $\underbrace{V^* \times V^* \times \cdots \times V^*}_d \rightarrow \mathbb{k}$ is canonically isomorphic to the space of linear maps $S^d V^* \rightarrow \mathbb{k}$.*

Corollary 11.2 *Under the assumptions of Proposition 11.2, an isomorphism of \mathbb{k} -algebras $\sigma : \mathbb{k}[x_0, x_1, \dots, x_n] \xrightarrow{\sim} SV^*$ is well defined by sending each basic monomial $x_0^{m_0} x_1^{m_1} \cdots x_n^{m_n} \in \mathbb{k}[x_0, x_1, \dots, x_n]$ to the basic commutative monomial $x_0^{m_0} x_1^{m_1} \cdots x_n^{m_n} \in SV^*$.*

Proof Since σ bijectively maps a basis to a basis, it is an isomorphism of vector spaces. Since σ respects multiplication of basis vectors, it is a homomorphism of algebras. \square

11.2.3 Polynomial Functions on an Affine Space

For every vector $v \in V$, there is well-defined homomorphism of \mathbb{k} -algebras

$$\text{ev}_v : SV^* \rightarrow \mathbb{k}, \quad a_1 a_2 \dots a_d \mapsto \prod_{v=1}^d \langle v, a_v \rangle, \quad (11.8)$$

which sends every commutative product of covectors to the product of their contractions with the vector $v \in V$. Indeed, we know that the map

$$\widetilde{\text{ev}}_p : V^* \times V^* \times \dots \times V^* \rightarrow \mathbb{k}, \quad a_1 a_2 \dots a_d \mapsto \prod_{v=1}^d \langle v, a_v \rangle, \quad (11.9)$$

is uniquely extended to a linear form $\mathcal{V}_d^* \rightarrow \mathbb{k}$, which annihilates the subspace $\mathcal{S}_n \subset \mathcal{V}_n^*$, because the map (11.9) is symmetric and multilinear. Therefore, it is consistently factorized through the linear form (11.8) on the quotient space $S^d V^* = \mathcal{V}_n^* / \mathcal{S}_n$.

If we fix a polynomial $f \in SV^*$ and let the vector v run through the vector space V , then we get a polynomial function

$$\tilde{f} : V \rightarrow \mathbb{k}, \quad v \mapsto f(v) = \text{ev}_v(f), \quad (11.10)$$

which is the polynomial function \tilde{f} considered at the very beginning of Sect. 11.2, when we chose a basis x_0, x_1, \dots, x_n in V^* and identified $\mathbb{k}[x_0, x_1, \dots, x_n]$ with SV^* by Corollary 11.2. Thus, the contraction map (11.8) agrees with evaluation of the polynomials in coordinates under any choice of coordinates in V .

11.2.4 Affine Algebraic Varieties

Every polynomial function $V \rightarrow \mathbb{k}$ can be viewed as a function $\mathbb{A}(V) \rightarrow \mathbb{k}$ on the affinization of V . Such a function is also called a *polynomial*. The zero set of a nonconstant polynomial function f on $\mathbb{A}(V)$ is denoted by

$$Z(f) \stackrel{\text{def}}{=} \{p \in \mathbb{A}(V) \mid f(p) = 0\}$$

and is called an *affine algebraic hypersurface* of degree $d = \deg f$. Intersections of algebraic hypersurfaces, i.e., solutions of arbitrary systems of polynomial equations, are called *affine algebraic varieties*. Affine subspaces, which are solutions of systems of linear equations, are the simplest examples of algebraic varieties.

11.3 Projective Algebraic Varieties

11.3.1 Homogeneous Equations

Typically, a nonconstant polynomial $f \in SV^* \setminus S^0V^*$ does not define a function on projective space $\mathbb{P}(V)$, because $f(v)$ usually varies as v runs through the 1-dimensional subspace located behind a point of $\mathbb{P}(V)$. However, for a *homogeneous* polynomial $f \in S^dV^*$ of arbitrary positive degree $d \in \mathbb{N}$, the zero set

$$Z(f) \stackrel{\text{def}}{=} \{v \in \mathbb{P}(V) \mid f(v) = 0\} \quad (11.11)$$

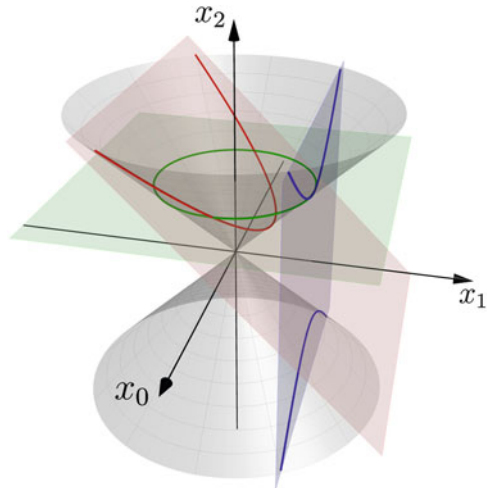
is still well defined, because the equations $f(v) = 0$ and $f(\lambda v) = \lambda^d f(v) = 0$ are equivalent. Geometrically, an affine hypersurface $Z(f) \subset \mathbb{A}(V)$ for homogeneous f is ruled by the lines passing through the origin, that is, it consists of the points of $\mathbb{P}(V)$. The zero set (11.11) considered as a figure within $\mathbb{P}(V)$ is called a *projective algebraic hypersurface* of degree $d = \deg f$. Let me stress that the notation $Z(f)$ in projective geometry always assumes that f is homogeneous of positive degree. Intersections of projective hypersurfaces, i.e., nonzero solutions of systems of homogeneous polynomial equations considered up to proportionality, are called *projective algebraic varieties*.

Example 11.3 (Projective Subspaces) The simplest examples of projective varieties are provided by the *projective subspaces* $\mathbb{P}(U) \subset \mathbb{P}(V)$ associated with vector subspaces $U \subset V$. They are given by systems of homogeneous linear equations $\xi(v) = 0$, where ξ runs through $\text{Ann}(U) \subset V^*$ or through some basis of $\text{Ann}(U)$. For example, for every pair of nonproportional vectors⁷ $a, b \in V$, there exists a unique projective line $(ab) \subset \mathbb{P}(V)$ passing through both a and b . Such a line is the projectivization of the 2-dimensional vector subspace spanned by a, b . It consists of nontrivial linear combinations $\lambda a + \mu b$, $\lambda, \mu \in \mathbb{k}$, considered up to proportionality. The ratio $(\lambda : \mu)$ can be used as an internal homogeneous coordinate within the line (ab) . On the other hand, the line (a, b) can be described by linear homogeneous equations $\xi(v) = 0$ in the unknown vector $v \in V$ for all $\xi \in \text{Ann}(a) \cap \text{Ann}(b) \subset V^*$.

Exercise 11.7 Show that for every affine chart $U_\xi \subset \mathbb{P}_n$ and k -dimensional projective subspace $K \subset \mathbb{P}_n$, either $K \cap U_\xi$ is empty or it is some k -dimensional affine subspace in U_ξ .

It follows from Proposition 6.3 on p. 139 that for every pair of projective subspaces $K, L \subset \mathbb{P}_n$, the inequality $\dim(K \cap L) \geq \dim K + \dim L - n$ holds. It implies, in particular, that every pair of lines in the projective plane intersect.

⁷That is, two distinct points of $\mathbb{P}(V)$.

Fig. 11.5 Real conic

Example 11.4 (Smooth Real Conic) The second-degree curve $C \subset \mathbb{P}_2 = \mathbb{P}(\mathbb{R}^3)$ given by the equation

$$x_0^2 + x_1^2 = x_2^2 \quad (11.12)$$

is called a *smooth real conic* (Fig. 11.5). In the standard chart U_1 , where $x_1 = 1$, in local affine coordinates $t_0 = x_0|_{U_1} = x_0/x_1$, $t_2 = x_2|_{U_1} = x_2/x_1$, equation (11.12) becomes the equation of a hyperbola, $t_2^2 - t_0^2 = 1$. In the standard chart U_2 , where $x_2 = 1$, in local coordinates $t_0 = x_0|_{U_2} = x_0/x_2$, $t_1 = x_1|_{U_2} = x_1/x_2$, it is the equation of a circle, $t_0^2 + t_1^2 = 1$. In the nonstandard chart $U_{x_1+x_2}$, where $x_1 + x_2 = 1$, in local affine coordinates $t = x_0|_{U_{x_1+x_2}} = x_0/(x_1 + x_2)$, $u = (x_2 - x_1)|_{U_{x_1+x_2}} = (x_2 - x_1)/(x_2 + x_1)$ we get⁸ the parabola $t^2 = u$. Thus, ellipse, parabola, and hyperbola are just different affine pieces of the same projective conic (11.12). The appearance of C in an affine chart depends on the positional relationship between C and the infinite line of the chart. Elliptic, parabolic, and hyperbolic shapes appear, respectively, when the infinite line does not intersect C , is tangent to C , and crosses C in two distinct points.

11.3.2 Projective Closure of an Affine Hypersurface

Consider the affine space \mathbb{A}^n as the standard affine chart U_0 within projective space \mathbb{P}_n . Then for every affine hypersurface $X = Z(f) \subset \mathbb{A}^n$ of degree $d = \deg f$, there exists a projective hypersurface $\bar{X} = Z(\bar{f}) \subset \mathbb{P}_n$ of the same degree

⁸Move x_1^2 to the right-hand side and divide both sides by $x_2 + x_1$.

$d = \deg \bar{f} = \deg f$ such that $\bar{X} \cap U_0 = X$. It is called the *projective closure* of X . If we expand f as a sum of homogeneous components $f = f_0 + f_1 + f_2 + \cdots + f_d$, where each f_i is homogeneous of degree i , then the homogeneous degree- d polynomial

$$\bar{f}(x_0, x_1, \dots, x_n) = f_0 \cdot x_0^d + f_1(x_1, x_2, \dots, x_n) \cdot x_0^{d-1} + \cdots + f_d(x_1, x_2, \dots, x_n)$$

is made from f by multiplication of each monomial by an appropriate power of x_0 , completing the total degree of the monomial up to d . The polynomial \bar{f} turns again into f for $x_0 = 1$:

$$f(x_1, x_2, \dots, x_n) = \bar{f}(1, x_1, x_2, \dots, x_n).$$

For example, the projective closure of the affine plane curve $x_1 = x_2^3$ is given by the homogeneous equation $x_0^2 x_1 = x_2^3$ and has just one infinite point $(0 : 1 : 0)$. In the standard affine chart U_1 , this projective cubic looks like the semicubic parabola $x_0^2 = x_2^3$ with a cusp at $(0 : 1 : 0)$.

In the general case, the complement $\bar{X} \setminus X = \bar{X} \cap U_0^{(\infty)}$ is a projective hypersurface within the infinitely distant hyperplane $x_0 = 0$. In homogeneous coordinates $(x_1 : x_2 : \cdots : x_n)$, it is given by the homogeneous equation $f_d(x_1, x_2, \dots, x_n) = 0$. In other words, the infinite points of \bar{X} are the zeros of the leading homogeneous form of f considered up to proportionality. In affine geometry, they are called the *asymptotic directions* of the affine variety $X = Z(f)$.

11.3.3 Space of Hypersurfaces

Since proportional equations have the same solution set, the projective hypersurfaces of degree d in $\mathbb{P}(V)$ can be treated as points of projective space $\mathbb{P}(S^d V^*)$, which is called the *space of degree- d hypersurfaces* in $\mathbb{P}(V)$.

Exercise 11.8 Find $\dim \mathbb{P}(S^d V^*)$.

It should be kept in mind that if the ground field is not algebraically closed, then some $f \in S^d V^*$ may determine nothing geometrically reminiscent of a hypersurface. For example, consider $Z(x_0^2 + x_1^2) = \emptyset$ on \mathbb{P}_1 over \mathbb{R} . Even over an algebraically closed field, some distinct points $f \neq g$ in $\mathbb{P}(S^d V^*)$ produce the same zero set $Z(f) = Z(g)$ in $\mathbb{P}(V)$. For example, the nonproportional polynomials $x_0^2 x_1$ and $x_0 x_1^2$ define the same two-point set $Z(f) = Z(g) = \{(1 : 0), (0 : 1)\}$ on \mathbb{P}_1 . Nevertheless, these geometric disharmonies can be overcome by passing to the algebraic closure and introducing multiplicities of components. The latter means that for $f = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, where p_1, p_2, \dots, p_k are different irreducible polynomials, we define $Z(f)$ to be the union of k components $Z(p_1), Z(p_2), \dots, Z(p_k)$ having multiplicities m_1, m_2, \dots, m_k . Thus, in the previous examples, $Z(x_0^2 + x_1^2)$ becomes

two points $(1 : \pm i)$ over \mathbb{C} , and $Z(x_0^2 x_1)$, $Z(x_0 x_1^2)$ become distinct, because $(1 : 0)$, $(0 : 1)$ appear in the first variety with multiplicities 1, 2, whereas in the second, they appear with multiplicities 2, 1. However, any strong explicit justification of a bijection between points of $\mathbb{P}(S^d V^*)$ and geometric objects in $\mathbb{P}(V)$ would take us too far afield. Let us postpone such a discussion to the second volume of this textbook.

11.3.4 Linear Systems of Hypersurfaces

For fixed $p \in \mathbb{P}(V)$, the relation $f(p) = 0$ is linear in $f \in S^d V^*$. Thus, the degree- d hypersurfaces $Z(f) \subset \mathbb{P}(V)$ passing through a given point p form a hyperplane in the space of hypersurfaces. A projective subspace within the space of hypersurfaces is called a *linear system* of hypersurfaces. All hypersurfaces in a linear system spanned by $Z(f_1)$, $Z(f_2)$, \dots , $Z(f_m)$ are given by equations of the form

$$\lambda_1 f_1 + \lambda_2 f_2 + \dots + \lambda_m f_m = 0, \text{ where } \lambda_1, \lambda_2, \dots, \lambda_m \in \mathbb{k}.$$

In particular, all these hypersurfaces contain the intersection

$$Z(f_1) \cap Z(f_2) \cap \dots \cap Z(f_m).$$

Traditionally, linear systems of dimensions 1, 2, and 3 are called *pencils*, *nets*, and *webs* respectively. Since every line in a projective space has nonempty intersection with every hyperplane, it follows that for every point, there is a hypersurface passing through that point in every pencil of hypersurfaces over an arbitrary ground field \mathbb{k} .

Example 11.5 (Pencils of Lines in a Plane) The lines in the projective plane $\mathbb{P}_2 = \mathbb{P}(V)$ are in bijection with the points of the *dual plane* $\mathbb{P}_2^\times = \mathbb{P}(V^*)$. Every 1-dimensional subspace $\mathbb{k} \cdot \xi \subset V^*$ produces the line $\mathbb{P}(\text{Ann} \xi) \subset \mathbb{P}(V)$, and the linear form ξ is recovered from the line uniquely up to proportionality. Conversely, every line in the dual plane \mathbb{P}_2^\times has the form $\mathbb{P}(\text{Ann} v)$ for some $v \in V$, unique up to proportionality, and it consists of all lines in \mathbb{P}_2 passing through the point $v \in \mathbb{P}_2$. Thus, every pencil of lines in \mathbb{P}_2 is the set of all lines passing through some point. This point is called the *center* of the pencil.

Example 11.6 (Collections of Points in \mathbb{P}_1 and Veronese Curves) Write U for the coordinate space \mathbb{k}^2 with coordinates $x_0, x_1 \in \mathbb{k}^{2*}$ and consider the projective line $\mathbb{P}_1 = \mathbb{P}(U)$. An unordered collection of d points (some of which may coincide)

$$p_1, p_2, \dots, p_d \in \mathbb{P}_1, \quad p_v = (p_{v,0} : p_{v,1}), \quad (11.13)$$

can be viewed as a projective hypersurface, the zero set of the homogeneous degree- d polynomial

$$f(x_0, x_1) = \prod_{v=1}^d \det(x, p_v) = \prod_{v=1}^d (p_{v,1}x_0 - p_{v,0}x_1). \quad (11.14)$$

By analogy with inhomogeneous polynomials $f(t) \in \mathbb{k}[t]$, whose roots are collections of points in \mathbb{A}_1 , we say that the points (11.13) are the *projective roots* of the homogeneous polynomial (11.14). Note that projective roots are defined only up to proportionality. In an affine chart whose infinity differs from all points (11.13), the factorization (11.14) is the usual factorization of an inhomogeneous polynomial in one variable provided by its roots.⁹ For example, if $p_{v,1} \neq 0$ for all v , then in the chart U_1 with local affine coordinate $t = x_0/x_1$, the factorization (11.14) can be rewritten as $f(t) = \text{const} \cdot \prod_{v=1}^d (t - \alpha_v)$, where $\alpha_v = p_{v,0}/p_{v,1}$ and $\text{const} = \prod_v p_{v,1}$, and in the chart U_1 with coordinate $s = 1/t$, the same factorization becomes $f(s) = \text{const} \cdot \prod_{v=1}^d (1 - \alpha_v s)$.

Every nonzero homogeneous polynomial of degree d in (x_0, x_1) certainly has at most d projective roots on \mathbb{P}_1 . If \mathbb{k} is algebraically closed, then there are exactly d roots counted with multiplicities, where the multiplicity of the root p means the number of factors proportional to $\det(t, p)$ in the irreducible factorization (11.14). We conclude that over an algebraically closed field \mathbb{k} , the unordered configurations of d points on \mathbb{P}_1 , in which some points may coincide, are in bijection with the points of the projective space $\mathbb{P}_d = \mathbb{P}(S^d U^*)$ of degree- d “hypersurfaces” in \mathbb{P}_1 .

Over a field \mathbb{k} , not necessarily algebraically closed, the configurations in which all d points coincide form a curve $C_d \subset \mathbb{P}_d = \mathbb{P}(S^d U^*)$ called the *degree- d Veronese curve* or *rational normal curve* of degree d . This curve can be viewed as the image of the *Veronese map*

$$\text{ver}_d : \mathbb{P}(U^*) \rightarrow \mathbb{P}(S^d U^*) , \quad \varphi \mapsto \varphi^d, \quad (11.15)$$

which sends a linear form $\varphi \in U^*$ to its d th power $\varphi^d \in S^d(U^*)$. Geometrically, φ is a linear equation of a point $p = \text{Ann } \varphi \in \mathbb{P}_1$, whereas the form φ^d has p as a projective root of multiplicity d .

Write linear forms $\varphi \in U^*$ as $\varphi(x) = \alpha_0 x_0 + \alpha_1 x_1$ and degree- d forms $f \in S^d(U^*)$ as $f(x) = \sum_v \binom{d}{v} \cdot a_v x_0^{d-v} x_1^v$. Let us use $(\alpha_0 : \alpha_1)$ and $(a_0 : a_1 : \dots : a_d)$ as homogeneous coordinates in $\mathbb{P}_1^\times = \mathbb{P}(U^*)$ and in $\mathbb{P}_d = \mathbb{P}(S^d U^*)$ respectively. Then the Veronese curve is described by the parametric equation

$$(\alpha_0 : \alpha_1) \mapsto (a_0 : a_1 : \dots : a_d) = (\alpha_0^d : \alpha_0^{d-1} \alpha_1 : \alpha_0^{d-2} \alpha_1^2 : \dots : \alpha_1^d). \quad (11.16)$$

⁹See Proposition 3.5 on p. 50.

We see that C_d consists of all points $(a_0 : a_1 : \cdots : a_d) \in \mathbb{P}_d$ whose coordinates form a geometric progression. This means that

$$\operatorname{rk} \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{d-2} & a_{d-1} \\ a_1 & a_2 & a_3 & \cdots & a_{d-1} & a_d \end{pmatrix} = 1,$$

and it is equivalent to a system of homogeneous quadratic equations $a_i a_j = a_{i+1} a_{j-1}$, which certify the vanishing of all 2×2 minors of the above matrix. Therefore the Veronese curve is in fact an algebraic variety. For example, the *Veronese conic* $C_2 \subset \mathbb{P}_2$ consists of all quadratic trinomials $a_0 x_0^2 + 2a_1 x_0 x_1 + a_2 x_1^2$ that are perfect squares of linear forms. It is given by the well-known quadratic equation

$$D/4 = -\det \begin{pmatrix} a_0 & a_1 \\ a_1 & a_2 \end{pmatrix} = a_1^2 - a_0 a_2 = 0 \quad (11.17)$$

and admits the parametric description

$$a_0 = \alpha_0^2, \quad a_1 = \alpha_0 \alpha_1, \quad a_2 = \alpha_1^2. \quad (11.18)$$

The rational normal curve (11.16) intersects every hyperplane defined by the linear equation

$$A_0 a_0 + A_1 a_1 + \cdots + A_d a_d = 0$$

precisely in the Veronese images $\operatorname{ver}_d((\alpha_0 : \alpha_1))$ of the projective roots $(\alpha_0 : \alpha_1) \in \mathbb{P}_1$ of the homogeneous polynomial $\sum A_v \cdot \alpha_0^{d-v} \alpha_1^v$ of degree d . Since the latter has at most d roots in \mathbb{P}_1 , no collection of $d + 1$ distinct points on the Veronese curve all lie on a hyperplane. Hence, for all k in the range $2 \leq k \leq d$, every collection of $k + 1$ distinct points on C_d are linearly generic, meaning that there is no $(k - 1)$ -dimensional projective subspace that contains them all. In particular, every triple of distinct points on C_d is noncollinear for all $d \geq 2$. Over an algebraically closed field \mathbb{k} of zero characteristic, the Veronese curve C_d intersects every hyperplane in exactly d points (some of which may coincide). This is the geometric reason for saying that C_d has degree d .

11.4 Complementary Subspaces and Projections

Projective subspaces $K = \mathbb{P}(U)$ and $L = \mathbb{P}(W)$ in $\mathbb{P}_n = \mathbb{P}(V)$ are called *complementary* if $K \cap L = \emptyset$ and $\dim K + \dim L = n - 1$. For example, two nonintersecting lines in \mathbb{P}_3 are always complementary. In the language of vectors, the complementarity of $\mathbb{P}(U)$ and $\mathbb{P}(W)$ in $\mathbb{P}(V)$ means that $V = U \oplus W$, because

of $U \cap V = \{0\}$ and

$$\dim U + \dim W = \dim K + 1 + \dim L + 1 = (n + 1) = \dim V.$$

In this case, every $v \in V$ admits a unique decomposition $v = u + w$, where $u \in U$, $w \in W$. If $v \notin U \cup W$, then both components u, w are nonzero. Geometrically, this means that for every point $v \notin K \sqcup L$, there exists a unique line $\ell = (uw)$ passing through v and intersecting both subspaces K, L in some point u, w . Therefore, every pair of complementary projective subspaces $K, L \subset \mathbb{P}_n$ produces a well-defined projection $\pi_L^K : (\mathbb{P}_n \setminus K) \rightarrow L$ from K onto L , which acts on L identically and sends every $v \in \mathbb{P}_n \setminus (K \sqcup L)$ to $w = (uw) \cap L$, where (uw) is the unique line passing through p and crossing K, L at some points u, w . In terms of homogeneous coordinates $(x_0 : x_1 : \dots : x_n)$ such that $(x_0 : x_1 : \dots : x_m)$ and $(x_{m+1} : x_{m+2} : \dots : x_n)$ are the coordinates within K and L respectively, the projection π_L^K just removes the first $(m + 1)$ coordinates.

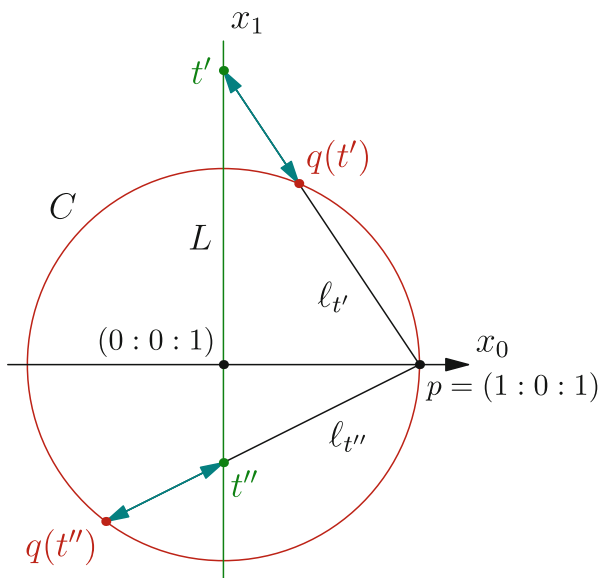


Fig. 11.6 Projection from $p \in C$ onto L

Example 11.7 (Projection of a Conic onto a Line) In Example 11.4, we considered the smooth conic C given in \mathbb{P}_2 by the homogeneous equation $x_0^2 + x_1^2 = x_2^2$. Let us project C from the point $p = (1 : 0 : 1) \in C$ on the line L given by the equation $x_0 = 0$. In the standard chart U_2 , where $x_2 = 1$, this projection $\pi_L^p : C \rightarrow L$ is shown in Fig. 11.6. It establishes a *birational bijection* between the conic and the

line, where birationality means that the coordinates of corresponding points $q = (q_0 : q_1 : q_2) \in C$, $t = (0 : t_1 : t_2) \in L$ are *rational functions* of each other:

$$\begin{aligned} (t_1 : t_2) &= (q_1 : (q_2 - q_0)), \\ (q_0 : q_1 : q_2) &= (t_1^2 - t_2^2) : 2t_1t_2 : (t_1^2 + t_2^2). \end{aligned} \quad (11.19)$$

The projection becomes bijective when we put $\pi_L^p(p)$ as the intersection point¹⁰ of L with the tangent line to C at p . All the lines passing through C are in bijection with the points of L , and every such line except for the tangent intersects C in exactly one point besides p .

Note that C can be transformed to the Veronese conic¹¹ $a_1^2 = a_0a_2$ by the invertible linear change of coordinates

$$\begin{cases} a_0 = x_2 + x_0, \\ a_1 = x_1, \\ a_2 = x_2 - x_0, \end{cases} \quad \begin{cases} x_0 = (a_0 - a_2)/2, \\ x_1 = a_1, \\ x_2 = (a_0 + a_2)/2. \end{cases}$$

Under this transformation, the rational parametrization (11.19) becomes the parametrization (11.18) of the Veronese conic.

11.5 Linear Projective Isomorphisms

11.5.1 Action of a Linear Isomorphism on Projective Space

Every linear isomorphism of vector spaces $F : U \xrightarrow{\sim} W$ induces a well-defined bijection $\bar{F} : \mathbb{P}(U) \xrightarrow{\sim} \mathbb{P}(W)$ called a *linear projective transformation* or an *isomorphism* of projective spaces $\mathbb{P}(U)$ and $\mathbb{P}(W)$.

Exercise 11.9 For two distinct hyperplanes $L_1, L_2 \subset \mathbb{P}_n$ and a point $p \notin L_1 \cup L_2$, show that the projection from p onto L_2 establishes an isomorphism of projective spaces $L_1 \xrightarrow{\sim} L_2$.

Theorem 11.1 *Let U and W be vector spaces of the same dimension $\dim U = \dim W = n + 1$. Given two ordered collections of $n + 2$ points $p_0, p_1, \dots, p_{n+1} \in \mathbb{P}(U)$, $q_0, q_1, \dots, q_{n+1} \in \mathbb{P}(W)$ such that no $n + 1$ points of each collection lie within a hyperplane, there exists a unique, up to proportionality, linear isomorphism $F : U \xrightarrow{\sim} W$ such that $\bar{F}(p_i) = q_i$ for all i .*

¹⁰In Fig. 11.6, the tangent line through p crosses L at the point $(0 : 1 : 0)$ lying at infinity.

¹¹See formula (11.17) on p. 268.

Proof Fix nonzero vectors u_i, w_i representing points p_i, q_i and use u_0, u_1, \dots, u_n and w_0, w_1, \dots, w_n as bases for U and W . The projective transformation $\bar{F} : \mathbb{P}(U) \rightarrow \mathbb{P}(W)$ induced by the linear map $F : U \rightarrow W$ takes p_0, p_1, \dots, p_n to q_0, q_1, \dots, q_n if and only if the matrix of F in our bases is nondegenerate diagonal. Write $\lambda_0, \lambda_1, \dots, \lambda_n$ for its diagonal elements and consider the remaining vectors $u_{n+1} = x_0 u_0 + x_1 u_1 + \dots + x_n u_n$ and $w_{n+1} = y_0 w_0 + y_1 w_1 + \dots + y_n w_n$. The condition $F(u_{n+1}) = \lambda_{n+1} w_{n+1}$ is equivalent to $n+1$ equalities $y_i = \lambda_{n+1} \lambda_i x_i$, $0 \leq i \leq n$, where each x_i is nonzero, because otherwise, $n+1$ points p_v with $v \neq i$ would lie in the hyperplane $x_i = 0$. For the same reason, each y_i is also nonzero. Thus, the diagonal elements $(\lambda_0, \lambda_1, \dots, \lambda_n) = \lambda_{n+1}^{-1} \cdot (y_1/x_1, y_2/x_2, \dots, y_n/x_n)$ are nonzero and unique up to a constant factor $\lambda_{n+1}^{-1} \neq 0$. \square

11.5.2 Linear Projective Group

The linear projective automorphisms of $\mathbb{P}(V)$ form a transformation group whose elements are linear automorphisms of V considered up to proportionality. This group is denoted by $\text{PGL}(V)$ and called the *linear projective group*. For the coordinate space $V = \mathbb{k}^{n+1}$, this group consists of proportionality classes of invertible square matrices and is denoted by $\text{PGL}_{n+1}(\mathbb{k})$.

Example 11.8 (Linear Fractional Transformations of a Line) The group $\text{PGL}_2(\mathbb{k})$ consists of nondegenerate 2×2 matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ considered up to proportionality. Such a matrix acts on the coordinate projective line $\mathbb{P}_1 = \mathbb{P}(\mathbb{k}^2)$ by the rule $(x_0 : x_1) \mapsto ((ax_0 + bx_1) : (cx_0 + dx_1))$. In the standard chart $U_1 \simeq \mathbb{A}^1$ with affine coordinate $t = x_0/x_1$, this action looks like the *linear fractional transformation*

$$t \mapsto \frac{at + b}{ct + d}.$$

This affine notation makes it obvious that proportional matrices produce the same transformation and that for every ordered triple of distinct points q, r, s , there exists a unique linear fractional transformation sending those points to $\infty, 0, 1$ respectively. It acts by the rule

$$t \mapsto \frac{t - r}{t - q} \cdot \frac{s - r}{s - q}. \quad (11.20)$$

11.6 Cross Ratio

The difference of affine coordinates $a = a_0/a_1$, $b = b_0/b_1$ of points $a = (a_0 : a_1)$, $b = (b_0 : b_1)$ on $\mathbb{P}_1 = \mathbb{P}(\mathbb{k}^2)$ up to a nonzero constant factor coincides with the determinant of the matrix of homogeneous coordinates of the points:

$$a - b = \frac{a_0}{a_1} - \frac{b_0}{b_1} = \frac{a_0 b_1 - a_1 b_0}{a_1 b_1} = \frac{\det(a, b)}{a_1 b_1}.$$

For every ordered quadruple of distinct points $p_1, p_2, p_3, p_4 \in \mathbb{P}_1$, the quantity

$$[p_1, p_2, p_3, p_4] \stackrel{\text{def}}{=} \frac{(p_1 - p_3)(p_2 - p_4)}{(p_1 - p_4)(p_2 - p_3)} = \frac{\det(p_1, p_3) \cdot \det(p_2, p_4)}{\det(p_1, p_4) \cdot \det(p_2, p_3)} \quad (11.21)$$

is called the *cross ratio* of the quadruple of points. Geometrically, the cross ratio $[p_1, p_2, p_3, p_4]$ considered as a point on $\mathbb{P}_1 = \mathbb{P}(\mathbb{k}^2)$ coincides with the image of p_4 under the linear fractional transformation (11.20) sending p_1, p_2, p_3 to $\infty, 0, 1$. Therefore, the cross ratio can take any value except for $\infty, 0, 1$, and one ordered quadruple of points can be transformed to another by a linear fractional map if and only if these quadruples have equal cross ratios.

Exercise 11.10 Verify the latter statement.

Since an invertible linear change of homogeneous coordinates on \mathbb{P}_1 is nothing but a projective automorphism of \mathbb{P}_1 , the right-hand side of (11.21) does not depend on the choice of homogeneous coordinates, and the middle part of (11.21), in which the cross ratio is expressed in terms of the differences of affine coordinates, depends neither on the choice of affine chart nor on the choice of local affine coordinate within the chart, assuming that all four points belong to the chart.¹²

11.6.1 Action of the Permutation Group S_4

Let us elucidate the behavior of the cross ratio under permutations of points. It is clear from (11.21) that a simultaneous transposition of two disjoint pairs of points does not change the cross ratio: $[p_1, p_2, p_3, p_4] = [p_2, p_1, p_4, p_3] = [p_3, p_4, p_2, p_1] = [p_4, p_3, p_2, p_1]$. Denote this quantity by ϑ . It is not hard to check

¹²That is, all numbers p_1, p_2, p_3, p_4 are finite.

that 24 permutations of points change ϑ as follows:

$$\begin{aligned}
 [p_1, p_2, p_3, p_4] &= [p_2, p_1, p_4, p_3] = [p_3, p_4, p_2, p_1] = [p_4, p_3, p_2, p_1] = \vartheta, \\
 [p_2, p_1, p_3, p_4] &= [p_1, p_2, p_4, p_3] = [p_3, p_4, p_1, p_2] = [p_4, p_3, p_1, p_2] = \frac{1}{\vartheta}, \\
 [p_3, p_2, p_1, p_4] &= [p_2, p_3, p_4, p_1] = [p_1, p_4, p_2, p_3] = [p_4, p_1, p_2, p_3] = \frac{\vartheta}{\vartheta - 1}, \\
 [p_4, p_2, p_3, p_1] &= [p_2, p_4, p_1, p_3] = [p_3, p_1, p_2, p_4] = [p_1, p_3, p_2, p_4] = 1 - \vartheta, \\
 [p_2, p_3, p_1, p_4] &= [p_3, p_2, p_4, p_1] = [p_1, p_4, p_3, p_2] = [p_4, p_1, p_3, p_2] = \frac{\vartheta - 1}{\vartheta}, \\
 [p_3, p_1, p_2, p_4] &= [p_1, p_3, p_4, p_2] = [p_2, p_4, p_1, p_3] = [p_4, p_2, p_1, p_3] = \frac{1}{1 - \vartheta},
 \end{aligned}
 \tag{11.22}$$

where we put in rows all permutations obtained by transposing disjoint pairs, respectively, in the identity permutation, in the transpositions $\sigma_{12}, \sigma_{13}, \sigma_{14}$, and in the cyclic permutations $\tau = (2, 3, 1, 4)$, $\tau^{-1} = (3, 1, 2, 4)$.

Exercise 11.11 Verify all the formulas (11.22). In particular, check that all 24 permutations of S_4 are listed there.

11.6.2 Special Quadruples of Points

It follows from formulas (11.22) that there are three special values $\vartheta = -1, 2, 1/2$ unchanged by the transpositions $\sigma_{12}, \sigma_{13}, \sigma_{14}$ and determined by the relations

$$\vartheta = \frac{1}{\vartheta}, \quad \vartheta = \frac{\vartheta}{\vartheta - 1}, \quad \vartheta = 1 - \vartheta.$$

The cycles $(2, 3, 1, 4), (3, 1, 2, 4)$ permute these three special values cyclically. Also, there are two special values of ϑ preserved by the cycles $(2, 3, 1, 4), (3, 1, 2, 4)$. They satisfy the quadratic equation

$$\vartheta^2 - \vartheta + 1 = 0 \iff \vartheta = \frac{\vartheta - 1}{\vartheta} \iff \vartheta = \frac{1}{1 - \vartheta}$$

and are equal to the cube roots of unity different from -1 , if they exist in \mathbb{k} . The transpositions $\sigma_{12}, \sigma_{13}, \sigma_{14}$ swap these special values of ϑ .

We say that an ordered quadruple of collinear points is *special* if its cross ratio equals one of the five special values of ϑ listed above. When we permute the points of a special quadruple, their cross ratio varies through either three or two

The lines in each pair are called *opposite sides* of the quadrangle $abcd$. The points a, b, c, d are called the *vertices* of the quadrangle. The opposite sides intersect at a triple of points

$$\begin{aligned} x &= (ab) \cap (cd), \\ y &= (ac) \cap (bd), \\ z &= (ad) \cap (bc). \end{aligned} \tag{11.24}$$

Three lines joining these points form an *associated triangle* of the quadrangle $abcd$. We claim that in the pencils of lines¹³ centered at x, y, z , two sides of the quadrangle are harmonic to two sides of the associated triangle. For the proof, let us identify the pencil of lines passing through x with lines (a, d) and (b, c) by taking the line $\ell \ni x$ to $\ell \cap (a, d)$ and $\ell \cap (b, c)$ respectively. Write $x' \in (a, d)$ and $x'' \in (b, c)$ for the points corresponding to (x, y) under this identification. We have to check that $[a, d, z, x'] = [b, c, z, x''] = -1$. Since the projections from x and from y establish linear projective isomorphisms between the lines (a, d) and (b, c) , we conclude that $[a, d, z, x'] = [b, c, z, x''] = [d, a, z, x']$. Since the cross ratio remains unchanged under swapping the first two points, it equals -1 .

Problems for Independent Solution to Chap. 11

Problem 11.1 Over the finite field of q elements, find the total number of k -dimensional (a) projective subspaces in \mathbb{P}_n , (b) affine subspaces in \mathbb{A}^n .

Problem 11.2 Formulate a geometric condition on a triple of lines ℓ_0, ℓ_1, ℓ_2 in $\mathbb{P}_2 = \mathbb{P}(V)$ necessary and sufficient for the existence of a basis x_0, x_1, x_2 in V^* such that each ℓ_i becomes the line at infinity for the standard affine chart $U_i = \{(x_0 : x_1 : x_2) \mid x_i \neq 0\}$ associated with this basis.

Problem 11.3 Choose points $A, B, C \in \mathbb{P}_2$ such that the points

$$A' = (1 : 0 : 0), \quad B' = (0 : 1 : 0), \quad C' = (0 : 0 : 1)$$

lie, respectively, on the lines (BC) , (CA) , (AB) and the three lines (AA') , (BB') , (CC') all pass through $(1 : 1 : 1)$.

Problem 11.4 Let the subset $\Phi \subset \mathbb{P}_n = \mathbb{P}(V)$ be visible as a k -dimensional affine subspace in every affine chart where it is visible at all (we assume that $k < n$ does not depend on the chart). Is it true that $\Phi = \mathbb{P}(W)$ for some $(k + 1)$ -dimensional vector subspace $W \subset V$?

¹³See Example 11.5 on p. 266.

Problem 11.5 Consider the following plane curves given by affine equations in the standard chart $U_0 \subset \mathbb{P}_2$: **(a)** $y = x^2$, **(b)** $y = x^3$, **(c)** $y^2 + (x - 1)^2 = 1$, **(d)** $y^2 = x^2(x + 1)$. Write their affine equations in two other standard charts U_1, U_2 and draw all 12 affine curves you deal with.

Problem 11.6 Consider the Euclidean plane \mathbb{R}^2 as a set of real points within the standard affine chart $U_0 \simeq \mathbb{C}^2$ in the complex projective plane $\mathbb{CP}_2 = \mathbb{P}(\mathbb{C}^3)$.

- (a)** Find two points $I_+, I_- \in \mathbb{CP}_2$ lying on all degree-2 curves visible within \mathbb{R}^2 as Euclidean circles.
- (b)** Let a curve C of degree 2 on \mathbb{CP}_2 pass through both points I_\pm and have at least three noncollinear points within \mathbb{R}^2 . Prove that $C \cap \mathbb{R}^2$ is a Euclidean circle.

Problem 11.7 In the notation of Example 11.7, show that (q_0, q_1, q_2) given by formula (11.19) on p. 270 as (t_1, t_2) runs through $\mathbb{Z} \times \mathbb{Z}$ enumerate all the proportionality classes of integer solutions of the Pythagorean equation $q_0^2 + q_1^2 = q_2^2$.

Problem 11.8 A nonidentical projective automorphism φ is called an *involution* if $\varphi^2 = \text{Id}$. Show that each involution of the projective line over an algebraically closed field has exactly two distinct fixed points.

Problem 11.9 (Projective Duality) Projective spaces $\mathbb{P}_n = \mathbb{P}(V)$ and $\mathbb{P}_n^\times = \mathbb{P}(V^*)$ are called *dual*. Show that each of them is the space of hyperplanes in the other. Prove that for each k in the range $0 \leq k \leq n - 1$, the assignment $\mathbb{P}(W) \leftrightarrow \mathbb{P}(\text{Ann}W)$ establishes a bijection between k -dimensional projective subspaces in \mathbb{P}_n and $(n - k - 1)$ -dimensional projective subspaces in \mathbb{P}_n^\times . Verify that this bijection reverses the inclusions of subspaces and takes a subspace $H \subset \mathbb{P}_n$ to the locus of all hyperplanes passing through H .

Problem 11.10 (Pappus's Theorem) Given two lines $\ell_1 \neq \ell_2$ on \mathbb{P}_2 and two triples of different points $a_1, b_1, c_1 \in \ell_1 \setminus \ell_2$ and $a_2, b_2, c_2 \in \ell_2 \setminus \ell_1$, show that the three points $(a_1b_2) \cap (a_2b_1)$, $(b_1c_2) \cap (b_2c_1)$, $(c_1a_2) \cap (c_2a_1)$ are collinear.

Problem 11.11 Formulate and prove a projectively dual version of Pappus's theorem.¹⁴

Problem 11.12 (Desargues's Theorem I) Given two triangles $A_1B_1C_1$ and $A_2B_2C_2$ on \mathbb{P}_2 , show that three points $(A_1B_1) \cap (A_2B_2)$, $(B_1C_1) \cap (B_2C_2)$, $(C_1A_1) \cap (C_2A_2)$ are collinear if and only if the three lines (A_1A_2) , (B_1B_2) , (C_1C_2) are concurrent.¹⁵ (Triangles possessing these properties are called *perspective*.)

Problem 11.13 (Desargues's Theorem II) Given three distinct points p, q, r on a line ℓ on \mathbb{P}_2 and three distinct points a, b, c outside the line, prove that the lines (ap) , (bq) , (cr) are concurrent if and only if there exists a linear projective

¹⁴That is, a statement about the annihilators of points and lines from Pappus's theorem that holds in \mathbb{P}_2^\times . It could start thus: "Given two distinct points and two triples of concurrent lines intersecting in these points. . ."

¹⁵This is, lie in the same pencil.

involution of the line ℓ exchanging p, q, r with the points $\ell \cap (bc), \ell \cap (ca), \ell \cap (ab)$, preserving the order.

Problem 11.14 Describe all linear fractional automorphisms $t \mapsto (at + b)/(ct + d)$

(a) preserving ∞ , (b) preserving both 0 and ∞ , (c) preserving 1 and swapping 0 and ∞ , (d) preserving 0 and swapping 1 and ∞ , (e) preserving ∞ and swapping 0 and 1.

Problem 11.15 Use the previous problem to obtain without any computations the equalities

$$[p_2, p_1, p_3, p_4] = [p_1, p_2, p_3, p_4]^{-1}, \quad [p_1, p_3, p_2, p_4] = 1 - [p_1, p_2, p_3, p_4],$$

$$[p_1, p_4, p_3, p_2] = ([p_1, p_2, p_3, p_4] - 1) / [p_1, p_2, p_3, p_4].$$

Problem 11.16 Prove that for five distinct points $p_1, p_2, \dots, p_5 \in \mathbb{P}_1$, one always has the equality

$$[p_1, p_2, p_3, p_4] \cdot [p_1, p_2, p_4, p_5] \cdot [p_1, p_2, p_5, p_3] = 1.$$

Problem 11.17 Prove that for eight distinct points $p_1, p_2, p_3, p_4, q_1, q_2, q_3, q_4 \in \mathbb{P}_1$, one always has the equality

$$[p_1, p_2, q_3, q_4] \cdot [p_2, p_3, q_1, q_4] \cdot [p_3, p_1, q_2, q_4]$$

$$\cdot [q_1, q_2, p_3, p_4] \cdot [q_2, q_3, p_1, p_4] \cdot [q_3, q_1, p_2, p_4] = 1.$$

Problem 11.18 Write U for the space of homogeneous linear forms in t_0, t_1 , and $\mathbb{P}_3 = \mathbb{P}(S^3 U)$ for the projectivization of the space of homogeneous cubic forms in t_0, t_1 . Describe the projections of the Veronese cubic¹⁶ $C_3 \subset \mathbb{P}_3$:

- (a) from the point t_0^3 in the plane spanned by $3 t_0^2 t_1, 3 t_0 t_1^2, t_1^3$;
- (b) from the point $3 t_0^2 t_1$ in the plane spanned by $t_0^3, 3 t_0 t_1^2, t_1^3$;
- (c) from point $t_0^3 + t_1^3$ in the plane spanned by $t_0^3, 3 t_0^2 t_1, 3 t_0 t_1^2$.

More precisely, write down an explicit homogeneous equation for each target curve and draw it in all three standard affine charts in the target plane.

Problem 11.19 (Rational Normal Curves) In the notation of Example 11.6 on p. 266, prove that the following curves C in $\mathbb{P}_d = \mathbb{P}(S^d U)$ are transformed to each other by an appropriate linear projective automorphisms of \mathbb{P}_d :

- (a) C is the image of the Veronese map $\text{ver}_d : \mathbb{P}(U) \rightarrow \mathbb{P}(S^d U), \varphi \mapsto \varphi^d$;
- (b) C is the image of an arbitrary map $F : \mathbb{P}(U) \rightarrow \mathbb{P}(S^d U)$ given in homogeneous coordinates by $(\alpha_0 : \alpha_1) \mapsto (f_0(\alpha) : f_1(\alpha) : \dots : f_d(\alpha))$, where $f_i(\alpha)$ are any

¹⁶See Example 11.6 on p. 266.

linearly independent homogeneous degree- d polynomials in $\alpha = (\alpha_0, \alpha_1)$;

(c) C is the image of the map $\mathbb{P}_1 \rightarrow \mathbb{P}_d$ given in homogeneous coordinates by

$$(\alpha_0 : \alpha_1) \mapsto \left(\frac{1}{\det(p_0, \alpha)} : \frac{1}{\det(p_1, \alpha)} : \cdots : \frac{1}{\det(p_d, \alpha)} \right),$$

where $p_0, p_1, \dots, p_d \in \mathbb{P}_1$ are arbitrarily fixed distinct points and $\det(a, b) = a_0b_1 - a_1b_0$ for $a = (a_0 : a_1), b = (b_0 : b_1) \in \mathbb{P}_1$.

(d) Fix $d + 3$ points $p_1, p_2, \dots, p_d, a, b, c \in \mathbb{P}_d$ such that no $(d + 1)$ of them lie within a hyperplane. Write $\ell_i \simeq \mathbb{P}_1 \subset \mathbb{P}_d^\times$ for a pencil of hypersurfaces passing through the $(n - 2)$ -dimensional subspace spanned by $n - 1$ points p_v with $v \neq i$. Let $\psi_{ij} : \ell_j \simeq \ell_i$ be the linear projective isomorphism that sends the three hyperplanes of ℓ_j passing through a, b, c to the three hyperplanes of ℓ_i passing through a, b, c respectively. The curve C is the locus of the intersection points of the n -tuples of the corresponding hyperplanes:

$$C = \bigcup_{H \in \ell_1} H \cap \psi_{21}(H) \cap \cdots \cap \psi_{n1}(H).$$

Problem 11.20 Show that for any $n + 3$ points in \mathbb{P}_n such that no $(n + 1)$ of them lie within a hyperplane, there exists a unique rational normal curve $C \subset \mathbb{P}_n$ from the previous problem that passes through all $n + 3$ given points.

Chapter 12

Groups

12.1 Definition and First Examples

A set G is called a *group* if it is equipped with a binary operation

$$G \times G \rightarrow G, \quad (g_1, g_2) \mapsto g_1 g_2,$$

called *composition*,¹ that satisfies the following three properties:

$$\text{associativity:} \quad \forall f, g, h \in G \quad (fg)h = f(gh), \quad (12.1)$$

$$\text{existence of unit:} \quad \exists e \in G : \forall g \in G, \quad eg = g, \quad (12.2)$$

$$\text{existence of inverse elements:} \quad \forall g \in G \quad \exists g^{-1} \in G : g^{-1}g = e. \quad (12.3)$$

For example, every multiplicative abelian group is a group satisfying one extra relation, commutativity: $fg = gf$ for all $f, g \in G$.

A map of groups $\varphi : S \rightarrow T$ is called a *group homomorphism* if $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in S$. In the context of groups, the terms *monomorphism*, *epimorphism*, and *isomorphism* mean a group homomorphism that respectively is injective, surjective, and bijective.

Exercise 12.1 Check that the composition of homomorphisms is a homomorphism.

The conditions (12.1)–(12.3) immediately imply some other expected properties of composition. The element g^{-1} in (12.3) that is a left inverse of g is automatically a right inverse. This follows from the equalities $g^{-1}gg^{-1} = eg^{-1} = g^{-1}$. Left multiplication of the left and right sides by the element that is a left inverse to g^{-1} leads to $gg^{-1} = e$. The element g^{-1} that is the inverse of g is uniquely determined

¹Sometimes also, depending on context, called multiplication, and sometimes, in the case of an abelian group, addition and denoted by $+$.

by g , because the equalities $fg = e$ and $gh = e$ imply $f = fe = f(gh) = (fg)h = eh = h$.

Exercise 12.2 Check that $(g_1 g_2 \cdots g_k)^{-1} = g_k^{-1} \cdots g_2^{-1} g_1^{-1}$.

The left unit e in (12.2) is also the right unit, because $ge = g(g^{-1}g) = (gg^{-1})g = eg = g$. This implies the uniqueness of the unit, because for two units e', e'' , the equalities $e' = e'e'' = e''$ hold.

For a finite group G , we write $|G|$ for the cardinality of G and call it the *order* of G . A subset $H \subset G$ is called a *subgroup* of G if H is a group with respect to the composition in G . The intersection of any set of subgroups is clearly a subgroup.

Exercise 12.3 Verify that $H \subset G$ is a subgroup if and only if $h_1 h_2^{-1} \in H$ for all $h_1, h_2 \in H$.

Example 12.1 (Transformation Groups) The main motivating examples of groups are the transformation groups. We have already met many such groups. The bijective endomorphisms $X \rightarrow X$ of a set X form a group, denoted by $\text{Aut } X$ and called the *automorphism group* of X . The automorphism group of a finite set $\{1, 2, \dots, n\}$ is the *symmetric group* S_n . Its order is given by $|S_n| = n!$. The even permutations form a subgroup $A_n \subset S_n$ of order $|A_n| = n!/2$. A *transformation group* of X is any subgroup $G \subset \text{Aut } X$. If a set X is equipped with some extra algebraic or geometric structure, then the set of all automorphisms of X respecting that structure forms a transformation group $G \subset \text{Aut } X$. In this way, we get *linear groups* acting on a vector space V : the general linear group $\text{GL}(V)$ of all *linear* automorphisms; the special linear group $\text{SL}(V)$ of volume-preserving linear automorphisms; the orthogonal group $\text{O}(V)$ of *isometries* of a Euclidean vector space V and its special subgroup $\text{SO}(V) = \text{O}(V) \cap \text{SL}(V)$; the projective linear group $\text{PGL}(V)$ of *linear projective* automorphisms of projective space $\mathbb{P}(V)$; etc. If $X = G$ is itself a group, we write $\text{Aut } G$ for the group of group automorphisms of G .

Exercise 12.4 Let G be the additive residue group $\mathbb{Z}/(p)$ for a prime $p \in \mathbb{N}$. Describe $\text{Aut } G$.

For a transformation g of a set X and an element $x \in X$, we will shorten the notation $g(x)$ to gx .

12.2 Cycles

12.2.1 Cyclic Subgroups

For a group G and element $g \in G$, we write $\langle g \rangle$ for the smallest subgroup in G containing g . It is called the *cyclic subgroup* spanned by g , because it is formed by all integer powers g^m , where we put $g^0 \stackrel{\text{def}}{=} e$ and $g^{-n} \stackrel{\text{def}}{=} (g^{-1})^n$ as usual. Therefore,

the group $\langle g \rangle$ is abelian, and there is a surjective homomorphism of abelian groups

$$\varphi_g : \mathbb{Z} \twoheadrightarrow \langle g \rangle, \quad m \mapsto g^m,$$

which takes addition to multiplication. If $\ker \varphi_g = 0$, then $\langle g \rangle \simeq \mathbb{Z}$, and all integer powers g^m are distinct. In this case, we say that g has *infinite order* and write $\text{ord } g = \infty$. If $\ker \varphi_g \neq 0$, then $\ker \varphi_g = (n)$ and $\langle g \rangle \simeq \mathbb{Z}/(n)$, where $n \in \mathbb{N}$ is the smallest positive exponent such that $g^n = e$. This exponent is called the *order* of the element g and is denoted by $\text{ord}(g)$. Note that the order of an element equals the order of the cyclic subgroup spanned by that element. If $\text{ord } g = n$, then all distinct elements of $\langle g \rangle$ are exhausted by $e = g^0, g = g^1, g^2, \dots, g^{n-1}$.

12.2.2 Cyclic Groups

An abstract group G is called *cyclic*² if $G = \langle g \rangle$ for some $g \in G$. Such an element g is called a *generator* of the cyclic group G . For example, the additive group of integers \mathbb{Z} is cyclic and has two generators, 1 and -1 . We have seen in Theorem 3.2 on p. 63 that every finite multiplicative subgroup of a field is cyclic. The additive group of residue classes $\mathbb{Z}/(n)$ is also cyclic and usually has many generators. For example, $\mathbb{Z}/(10)$ is generated by each of the four classes $[\pm 1]_6, [\pm 3]_6$ and by none of the six remaining classes.

Lemma 12.1 *An element $h = g^k$ generates the cyclic group $\langle g \rangle$ of order n if and only if $\text{GCD}(k, n) = 1$.*

Proof Since $\langle h \rangle \subset \langle g \rangle$, the coincidence $\langle h \rangle = \langle g \rangle$ is equivalent to the inequality $\text{ord } h \geq n$. The equality $h^m = g^{mk} = e$ holds if and only if $n \mid mk$. If $\text{GCD}(n, k) = 1$, then $n \mid mk$ only if $n \mid m$, which forces $\text{ord } h \geq n$. If $n = n_1 d$ and $k = k_1 d$ for some integer $d > 1$, then $h^{n_1} = g^{k n_1} = g^{n k_1} = e$, that is, $\text{ord } h \leq n_1 < n$. \square

12.2.3 Cyclic Type of Permutation

A permutation $\tau \in S_n$ is called a *cycle*³ of length m if it acts on some m elements⁴ $i_1, i_2, \dots, i_m \in \{1, 2, \dots, n\}$ as

$$i_1 \mapsto i_2 \mapsto \dots \mapsto i_{m-1} \mapsto i_m \mapsto i_1 \quad (12.4)$$

²See Sect. 3.6.1 on p. 62.

³Or a *cyclic permutation*.

⁴Not necessarily sequential or increasing.

and leaves all the other elements fixed. In this case, we write $\tau = |i_1, i_2, \dots, i_m|$. The notation is indicative but not quite correct: the same cycle (12.4) permits m distinct expressions $|i_1, i_2, \dots, i_m|$ obtained from each other by cyclic permutations of the indices.

Exercise 12.5 How many different cycles of length m are there in S_n ?

Exercise 12.6 Check that $|i_1, i_2, \dots, i_m|^k$ is a cycle if and only if $\text{GCD}(k, m) = 1$.

Theorem 12.1 *Every permutation is a composition of disjoint (and therefore commuting) cycles. Such a decomposition is unique up to permutation of the factors.*

Proof Since the set $X = \{1, 2, \dots, n\}$ is finite, for every $x \in X$ and $g \in S_n$, there must be repetitions in the infinite sequence $x \xrightarrow{g} gx \xrightarrow{g} g^2x \xrightarrow{g} g^3x \xrightarrow{g} \dots$. Since g is bijective, the leftmost repeated element is x . Therefore, under iterations of g , each point $x \in X$ goes through some cycle. Two such cycles beginning from different points x, y either coincide or do not intersect each other at all, because g is bijective. \square

Exercise 12.7 Show that two cycles $\tau_1, \tau_2 \in S_n$ commute in exactly two cases: (1) they are disjoint; (2) they are of the same length m and $\tau_1 = \tau_2^s$ for some s coprime to m .

Definition 12.1 (Cyclic Type of Permutation) Let a permutation $g \in S_n$ be a composition of disjoint cycles $\tau_1, \tau_2, \dots, \tau_s$ numbered in nonincreasing order of their lengths $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$ including all cycles of length 1 (corresponding to fixed elements of g). The Young diagram $\lambda(g)$ formed by the rows of lengths $\lambda_1, \lambda_2, \dots, \lambda_k$ is called a *cyclic type* of the permutation g . Note that this Young diagram consists of $|\lambda| = n$ cells.

Example 12.2 The permutation $g = (6, 5, 4, 1, 8, 3, 9, 2, 7) \in S_9$ can be decomposed into disjoint cycles as

$$g = |1, 6, 3, 4| |2, 5, 8| |7, 9| \quad \text{and has} \quad \lambda(g) = \begin{array}{|c|c|c|c|} \hline \square & \square & \square & \square \\ \hline \square & \square & \square & \square \\ \hline \square & \square & \square & \square \\ \hline \end{array}.$$

If we write the contents of the cycles in the rows of a Young diagram, we see that there may be different permutations of the same cyclic type. For example, the permutations

$$g = \begin{array}{|c|c|c|c|} \hline 1 & 6 & 3 & 4 \\ \hline 2 & 5 & 8 & \\ \hline 7 & 9 & & \\ \hline \end{array} \quad \text{and} \quad g' = \begin{array}{|c|c|c|c|} \hline 7 & 9 & 3 & 4 \\ \hline 2 & 5 & 8 & \\ \hline 1 & 6 & & \\ \hline \end{array}$$

certainly are different. There are altogether $(n-1)!$ different maximal cycles of length n , which have cyclic type $\lambda = (n)$ (one row of width n). The only permutation of cyclic type $\lambda = 1^n \stackrel{\text{def}}{=} (1, 1, \dots, 1)$ (one column of height n) is the identity.

Exercise 12.8 Write $m_i = m_i(\lambda)$ for the number of rows of length i in the Young diagram λ . Therefore, $0 \leq m_i \leq |\lambda|$ for each i and $\sum_i i \cdot m_i = |\lambda| = n$. Show that the total number of distinct permutations of cyclic type λ in S_n is equal⁵ to

$$\frac{n!}{\prod_i i^{m_i} \cdot m_i!}.$$

Example 12.3 (How to Compute Order and Sign) The order of a permutation of cyclic type $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_s)$ is equal to $\text{LCM}(\lambda_1, \lambda_2, \dots, \lambda_s)$. For example, the permutation

$$\begin{aligned} & (3, 12, 7, 9, 10, 4, 11, 1, 6, 2, 8, 5) \\ &= |1, 3, 7, 11, 8| |2, 12, 5, 10| |4, 9, 6| \in S_{12} \end{aligned}$$

has order $5 \cdot 4 \cdot 3 = 60$. The thread rule⁶ shows that the sign of a cycle of length m equals $(-1)^{m-1}$. Hence a permutation is even if and only if it has an even number of even-length cycles.

Exercise 12.9 Calculate $\text{sgn}(g)$ and g^{15} for $g = (6, 5, 4, 1, 8, 3, 9, 2, 7) \in S_9$.

12.3 Groups of Figures

For each figure Φ in Euclidean space \mathbb{R}^n , the bijective maps $\Phi \rightarrow \Phi$ induced by the orthogonal⁷ linear maps $F : \mathbb{R}^n \rightarrow \mathbb{R}^n$ such that $F(\Phi) = \Phi$ form a transformation group of Φ . This group is called the *complete group of the figure* Φ and is denoted by O_Φ . The subgroup $SO_\Phi \subset O_\Phi$ formed from the bijections induced by the proper⁸ orthogonal maps $\mathbb{R}^n \rightarrow \mathbb{R}^n$ is called the *proper group of the figure*. If Φ lies within some hyperplane $\Pi \subset \mathbb{R}^n$, then the complete and proper groups coincide, because every nonproper isometry F composed with an orthogonal reflection in Π becomes proper but has the same restriction on Π as F .

Exercise 12.10 Make models of the five Platonic solids: tetrahedron, octahedron, cube, dodecahedron, and icosahedron.⁹

⁵Compare with formula (1.11) on p. 7.

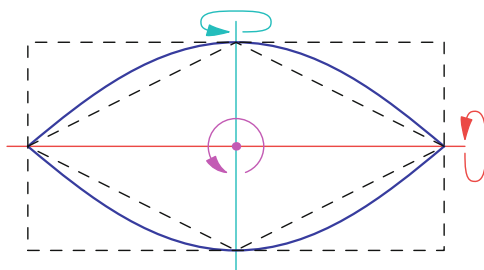
⁶See Example 9.2 on p. 209.

⁷See Sect. 10.5 on p. 244.

⁸That is, orientation-preserving (see Sect. 10.5 on p. 244).

⁹See Figs. 12.5, 12.6, 12.7, 12.8 on p. 288.

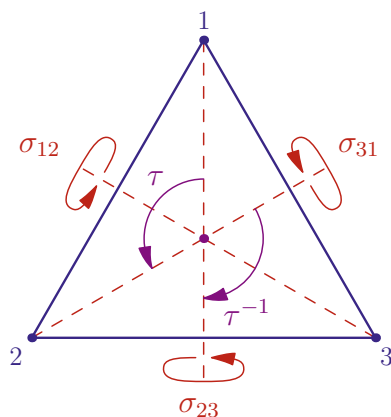
Fig. 12.1 The dihedral group D_2



Example 12.4 (Dihedral Groups D_n) Consider a regular plane n -gon placed within \mathbb{R}^3 in such a way that its center is at the origin. The group of such an n -gon is denoted¹⁰ by D_n and called the n th dihedral group. The simplest dihedron has $n = 2$ and looks like an oblong lune with two vertices, two edges, and two faces as shown in Fig. 12.1. The group D_2 of such a lune is the same as the group of a circumscribed rectangle or the group of an inscribed rhombus, assuming that both are not squares. The group D_2 consists of the identity map and three rotations by 180° about mutually perpendicular axes: one joins the vertices, another joins the midpoints of edges, and the third is perpendicular to the plane of the dihedron and passes through its center. The group D_2 is also known as the *Klein four group* and is often denoted by V_4 .

Exercise 12.11 Verify that $D_2 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

Fig. 12.2 Group of a triangle



¹⁰In many textbooks, this group is denoted by D_{2n} to emphasize its order, but we prefer to stress its geometric origin.

Next, for $n = 3$, we get the *group of the triangle* D_3 of order 6. It consists of the identity map, two rotations τ, τ^{-1} by $\pm 120^\circ$ about the center, and three reflections¹¹ σ_{ij} in the medians of the triangle (see Fig. 12.2). Since an isometry $\mathbb{R}^2 \mapsto \mathbb{R}^2$ is uniquely determined by its action on the vertices of an equilateral triangle centered at the origin, the triangle group D_3 is isomorphic to the permutation group S_3 of the vertices. Under this isomorphism, rotations by $\pm 120^\circ$ are identified with the mutually inverse cycles $(2, 3, 1), (3, 1, 2)$, while reflections are identified with the transpositions $\sigma_{23} = (1, 3, 2), \sigma_{13} = (3, 2, 1), \sigma_{12} = (2, 1, 3)$.

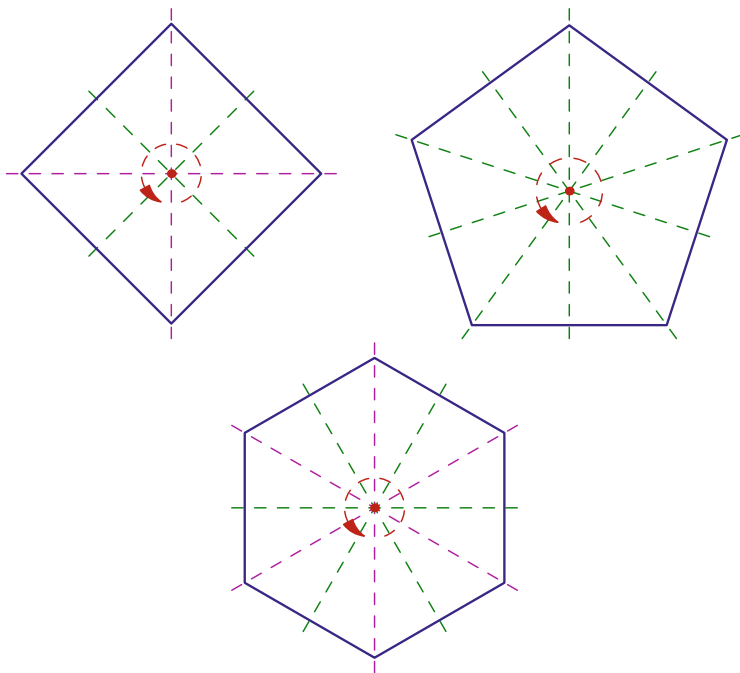


Fig. 12.3 Dihedral reflection axes for D_4, D_5, D_6

Since an isometry $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ is uniquely determined by its action on the affine coordinate system formed by some vertex and two basis vectors drawn along the outgoing edges from this vertex, the dihedral group D_n has order $|D_n| = 2n$ for all $n \geq 2$: the chosen vertex can be mapped to any one of n vertices, whereupon we have two ways of mapping the basis vectors. The resulting $2n$ maps are exhausted by the n rotations about the center of the dihedron by angles $2\pi k/n$, where $0 \leq k \leq n-1$ (for $k = 0$ we get the identity map), and n reflections¹² in the lines joining a vertex

¹¹Which also may be treated as rotations by 180° about the medians.

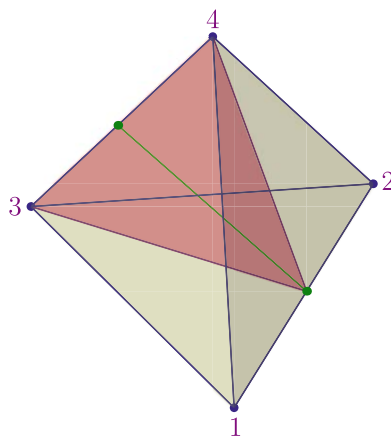
¹²Or rotations by 180° in the space \mathbb{R}^3 .

with the midpoint of the opposite edge for odd n and joining either opposite vertices or midpoints of opposite edges for even n (see Fig. 12.3).

Exercise 12.12 Write multiplication tables for the groups D_3 , D_4 , D_5 similar to the one presented in formula (1.20) on p. 11.

Example 12.5 (Groups of the Tetrahedron) Consider a regular tetrahedron centered at the origin of \mathbb{R}^3 . Since an isometry of \mathbb{R}^3 is uniquely determined by its action on the vertices of the tetrahedron and this action can be chosen arbitrarily, the complete group of the regular tetrahedron O_{tet} is isomorphic to the permutation group S_4 of the vertices. In particular, $|O_{\text{tet}}| = |S_4| = 24$. The proper tetrahedral group SO_{tet} consists of $12 = 4 \cdot 3$ transformations. Indeed, a rotation of the tetrahedron is uniquely determined by its action on the affine coordinate system formed by a vertex and the outgoing three edges from it. The vertex can be mapped to any one of four vertices, whereupon we have exactly three possibilities for an orientation-preserving superposition of edges. The resulting 12 rotations are the identity, $4 \cdot 2 = 8$ rotations by $\pm 120^\circ$ about the axes joining a vertex with the center of the opposite face, and three rotations by 180° about the axes joining the midpoints of opposite edges (see Fig. 12.4).

Fig. 12.4 Reflection plane σ_{12} and axis of 180° rotation $\sigma_{12}\sigma_{34}$



The complete tetrahedral group consists of the 12 rotations just listed, 6 reflections σ_{ij} in the planes passing through the midpoint of the edge $[i, j]$ and the opposite edge, and 6 more improper transformations corresponding to 6 cyclic permutations of vertices: $|1234\rangle$, $|1243\rangle$, $|1324\rangle$, $|1342\rangle$, $|1423\rangle$, $|1432\rangle$. Any such 4-cycle can be realized as a rotation by $\pm 90^\circ$ about the axis joining the midpoints of opposite edges followed by a reflection in the plane perpendicular to the axis and passing through the center of the tetrahedron.

Exercise 12.13 Write each 4-cycle as a composition of reflections σ_{ij} .

Exercise 12.14 Check that the isomorphism $O_{\text{tet}} \cong S_4$ takes reflections σ_{ij} to transpositions $|ij\rangle$; rotations by $\pm 120^\circ$ (i.e., compositions $\sigma_{ij}\sigma_{jk}$ for different i, j, k) to cycles $|ijk\rangle$; rotations by $\pm 180^\circ$ to three pairs of simultaneous transpositions in disjoint pairs $\sigma_{12}\sigma_{34} = (2, 1, 4, 3)$, $\sigma_{13}\sigma_{24} = (3, 4, 1, 2)$, $\sigma_{14}\sigma_{23} = (4, 3, 2, 1)$ of cyclic type $\begin{smallmatrix} \square & \square \\ \square & \square \end{smallmatrix}$. Convince yourself that the latter triple of involutions together with the identity forms the Klein four group $V_4 \cong D_2$.

Example 12.6 (Groups of the Dodecahedron) As in the previous example, each rotation of a regular dodecahedron is uniquely determined by its action on the affine coordinate system formed by some vertex and the triple of outgoing edges. We can move the vertex to any one of 20 dodecahedral vertices, whereupon there are three ways for an orientation-preserving superposition of edges. Therefore, the proper group of the dodecahedron consists of $20 \cdot 3 = 60$ rotations: $6 \cdot 4 = 24$ rotations by angles $2\pi k/5$, $1 \leq k \leq 4$ about axes joining the centers of opposite faces, $10 \cdot 2 = 20$ rotations by angles $\pm 2\pi/3$ about axes joining opposite vertices, 15 rotations by angles 180° about axes joining the midpoints of opposite edges (see Fig. 12.5), and the identity. The complete group of the dodecahedron has cardinality $20 \cdot 6 = 120$. Besides the 60 rotations just listed, it contains their compositions with the central symmetry in the origin $-\text{Id} : \mathbb{R}^3 \rightarrow \mathbb{R}^3, v \mapsto -v$.

Exercise 12.15 Show that the orders of the complete groups of the cube, octahedron, and icosahedron (Figs. 12.6, 12.7, and 12.8) are equal to 48, 48, and 120 respectively. Check that the corresponding proper groups consist of 24, 24, and 60 rotations and list them all.

Fig. 12.5 Dodecahedron

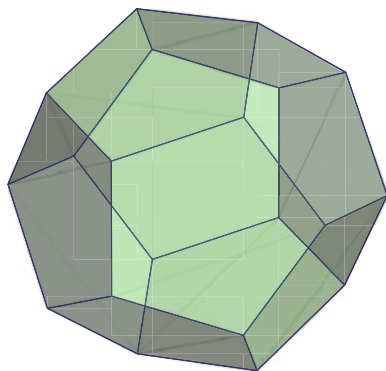
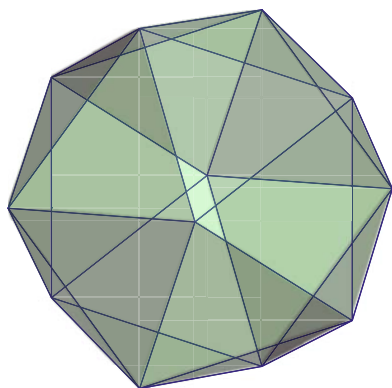
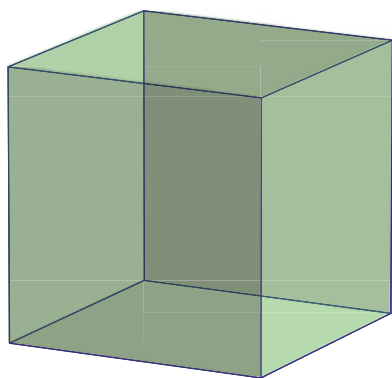
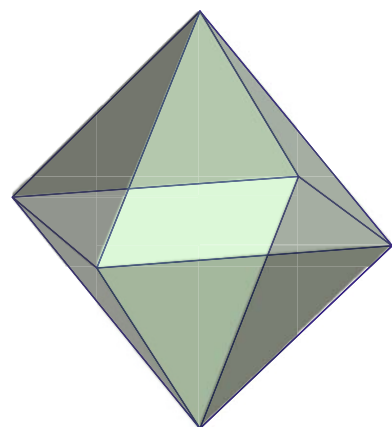


Fig. 12.6 Icosahedron**Fig. 12.7** Cube**Fig. 12.8** Octahedron

12.4 Homomorphisms of Groups

Homomorphisms of arbitrary groups share the key properties of the abelian group homomorphisms considered in Sect. 2.6 on p. 31. Namely, a homomorphism

$$\varphi : G_1 \rightarrow G_2$$

sends the unit $e_1 \in G_1$ to the unit $e_2 \in G_2$. This follows from the equalities

$$\varphi(e_1)\varphi(e_1) = \varphi(e_1e_1) = \varphi(e_1)$$

after multiplication of the left and right sides by $\varphi(e_1)^{-1}$. Further, $\varphi(g^{-1}) = \varphi(g)^{-1}$ for every $g \in G$, because $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_1) = e_2$. Therefore, the image $\text{im } \varphi \stackrel{\text{def}}{=} \varphi(G_1) \subset G_2$ of a group homomorphism is a subgroup in the target group. As for abelian groups, the preimage of the unit is called the *kernel* of the homomorphism and is denoted by

$$\ker \varphi \stackrel{\text{def}}{=} \varphi^{-1}(e_2) = \{g \in G_1 \mid \varphi(g) = e_2\}.$$

The kernel is a subgroup of G_1 by Exercise 12.3, because for all $g, h \in \ker \varphi$, we have

$$\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} = e_2e_2 = e_2.$$

The set-theoretic structure of the other fibers is also the same as in the abelian case.

Proposition 12.1 *All nonempty fibers of a group homomorphism $\varphi : G_1 \rightarrow G_2$ are in bijection with $\ker \varphi$. Namely, $\varphi^{-1}(\varphi(g)) = g \cdot (\ker \varphi) = (\ker \varphi) \cdot g$ for every $g \in G_1$, where $g \cdot (\ker \varphi) \stackrel{\text{def}}{=} \{gh \mid h \in \ker \varphi\}$ and $(\ker \varphi) \cdot g \stackrel{\text{def}}{=} \{hg \mid h \in \ker \varphi\}$.*

Proof If $\varphi(t) = \varphi(g)$, then $\varphi(tg^{-1}) = \varphi(t)\varphi(g)^{-1} = e$ and $\varphi(g^{-1}t) = \varphi(g)^{-1}\varphi(t) = e$. Hence, $tg^{-1} \in \ker \varphi$ and $g^{-1}t \in \ker \varphi$. Therefore, t lies in both sets $(\ker \varphi) \cdot g$ and $g \cdot (\ker \varphi)$. Conversely, for all $h \in \ker \varphi$, we have $\varphi(hg) = \varphi(h)\varphi(g) = \varphi(g)$ and $\varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)$. Hence, for every $g \in G_1$, the fiber $\varphi^{-1}(\varphi(g))$ coincides with both sets $(\ker \varphi) \cdot g$ and $g \cdot (\ker \varphi)$. This forces $(\ker \varphi) \cdot g = g \cdot (\ker \varphi)$. Inverse bijections between $\varphi^{-1}(\varphi(g)) = g \cdot (\ker \varphi)$ and $\ker \varphi$ are provided by the maps

$$\begin{array}{ccc} \ker \varphi & \xrightleftharpoons[g^{-1}t \leftarrow t]{h \mapsto gh} & g \cdot (\ker \varphi) \end{array}$$

□

Corollary 12.1 *A group homomorphism $\varphi : G_1 \rightarrow G_2$ is injective if and only if $\ker \varphi = \{e\}$.*

□

Corollary 12.2 *For every finite group G and group homomorphism $\varphi : G \rightarrow H$, the equality*

$$|\operatorname{im}(\varphi)| = |G|/|\ker(\varphi)|$$

holds. In particular, both $|\ker \varphi|$ and $|\operatorname{im} \varphi|$ divide $|G|$. \square

Example 12.7 (Sign Homomorphism) In Corollary 9.1 on p. 209, we constructed the sign homomorphism $\operatorname{sgn} : S_n \rightarrow \{\pm 1\}$ from the symmetric group to the multiplicative group of signs.¹³ Its kernel is the group of even permutations $A_n = \ker \operatorname{sgn}$ of order $|A_n| = n!/2$.

Example 12.8 (Determinant and Finite Linear Groups) In Sect. 9.3.2 on p. 214 we constructed the determinant homomorphism

$$\det : \operatorname{GL}(V) \rightarrow \mathbb{k}^*, \quad F \mapsto \det F, \quad (12.5)$$

from the general linear group $\operatorname{GL}(V)$ of a vector space V to the multiplicative group \mathbb{k}^* of the ground field \mathbb{k} . The kernel of the determinant homomorphism is the special linear group

$$\operatorname{SL}(V) = \ker \det = \{F \in \operatorname{GL}(V) \mid \det F = 1\}.$$

If $\dim V = n$ and $\mathbb{k} = \mathbb{F}_q$ consists of q elements, the group $\operatorname{GL}(V)$ is finite of order

$$|\operatorname{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}),$$

because the elements of $\operatorname{GL}(V)$ are in bijection with the bases of V .

Exercise 12.16 Check this.

Since the determinant homomorphism (12.5) is surjective,¹⁴ the special linear group has order $|\operatorname{SL}_n(\mathbb{F}_q)| = |\operatorname{GL}_n(\mathbb{F}_q)|/|\mathbb{k}^*| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})/(q - 1)$.

Example 12.9 (Homomorphism of Linear Group to Projective Group) In Sect. 11.5 on p. 270, we have seen that every linear automorphism $F \in \operatorname{GL}(V)$ induces a bijective transformation $\overline{F} : \mathbb{P}(V) \rightarrow \mathbb{P}(V)$. This gives a surjective homomorphism

$$\pi : \operatorname{GL}(V) \twoheadrightarrow \operatorname{PGL}(V), \quad F \mapsto \overline{F}. \quad (12.6)$$

By Theorem 11.1 on p. 270, its kernel $\ker \pi \simeq \mathbb{k}^*$ consists of the *scalar homotheties* $v \mapsto \lambda v$, $\lambda \in \mathbb{k}^*$. The proportionality classes of volume-preserving operators form a subgroup called the *special projective group* and denoted by $\operatorname{PSL}(V) \subset \operatorname{PGL}(V)$.

¹³It is isomorphic to the additive group $\mathbb{Z}/(2)$ by taking $1 \mapsto 0$, $-1 \mapsto 1$.

¹⁴The diagonal matrix F with diagonal elements $(\lambda, 1, 1, \dots, 1)$ has $\det F = \lambda$.

Restricting the surjection (12.6) to the subgroup $\mathrm{SL}(V) \subset \mathrm{GL}(V)$, we get a surjective homomorphism

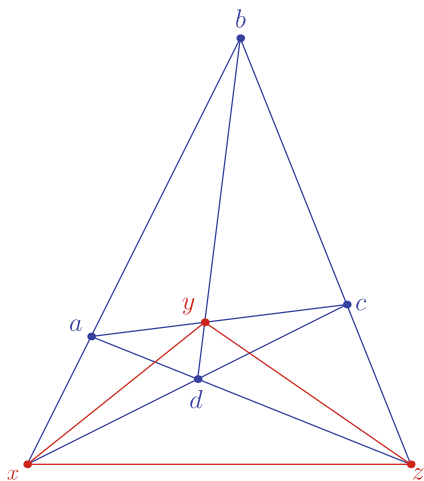
$$\pi' : \mathrm{SL}(V) \twoheadrightarrow \mathrm{PSL}(V), \quad F \mapsto \overline{F}, \quad (12.7)$$

with finite kernel isomorphic to the multiplicative group $\mu_n(\mathbb{k}) = \{\zeta \in \mathbb{k}^* \mid \zeta^n = 1\}$ of n th roots of unity in \mathbb{k} .

Example 12.10 (Surjection $S_4 \twoheadrightarrow S_3$) In Example 11.9 on p. 274 we attached a *complete quadrangle* $abcd$ to a quadruple of points $a, b, c, d \in \mathbb{P}_2$ such that no three of them are collinear. It is formed by three pairs of *opposite edges* (ab) and (cd) , (ac) and (bd) , (ad) and (bc) (see Fig. 12.9) crossing in a triple of points

$$x = (ab) \cap (cd), \quad y = (ac) \cap (bd), \quad z = (ad) \cap (bc), \quad (12.8)$$

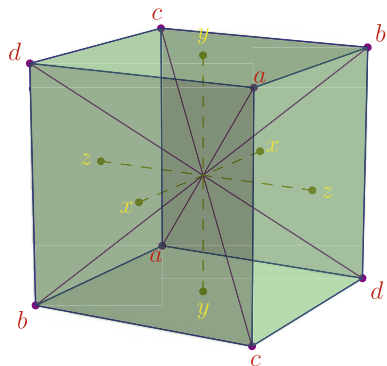
Fig. 12.9 Quadrangle and associated triangle



which form the *associated triangle* of the quadrangle $abcd$. Each permutation of the vertices a, b, c, d uniquely defines¹⁵ a projective linear automorphism of \mathbb{P}_2 sending the quadrangle to itself. We get an injective homomorphism $S_4 \hookrightarrow \mathrm{PGL}_3(\mathbb{k})$, whose image acts on the quadrangle $abcd$ and on the associated triangle xyz permuting the vertices x, y, z in accordance with the incidences (12.8). For example, the 3-cycle $(b, c, a, d) \in S_4$ leads to the cyclic permutation (y, z, x) ; the transpositions (b, a, c, d) , (a, c, b, d) , (c, b, a, d) lead to the transpositions (x, z, y) , (y, x, z) , (z, y, x) respectively. Therefore, we get a surjective homomorphism $S_4 \twoheadrightarrow S_3$. Its kernel has order $4!/3! = 4$ and coincides with the Klein four group formed by the identity map and three pairs of transpositions in disjoint pairs: (b, a, d, c) , (c, d, a, b) , (d, c, b, a) .

¹⁵See Theorem 11.1 on p. 270.

Fig. 12.10 From cube to quadrangle

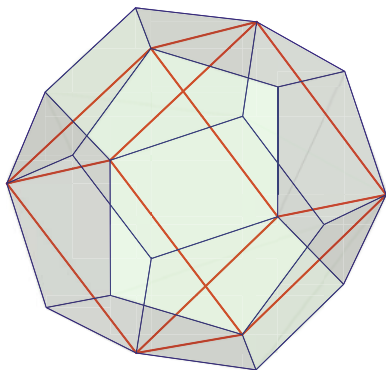


Example 12.11 (Proper Group of Cube and S_4) The proper group of the cube $SO_{\text{cube}} \subset SO_3(\mathbb{R})$ acts on the four lines a, b, c, d joining opposite vertices and on the three lines x, y, z joining the centers of opposite faces (see Fig. 12.10). On the projective plane $\mathbb{P}_2 = \mathbb{P}(\mathbb{R}^3)$, these seven lines become the vertices of the quadrangle $abcd$ and associated triangle xyz (see Fig. 12.9). Rotation by 180° about an axis joining the midpoints of opposite edges of the cube swaps the two diagonals joining the endpoints of these edges and takes each of the two remaining diagonals to itself. Since all transpositions of diagonals are achieved by rotations of the cube, we have a surjective homomorphism

$$SO_{\text{cube}} \rightarrow S_4. \quad (12.9)$$

It is bijective, because both groups are of the same order 24. Under the isomorphism (12.9), six rotations by $\pm 90^\circ$ about lines x, y, z go to six 4-cycles of cyclic type $\square\square\square\square$, three rotations by 180° about the same lines go to three pairs of disjoint transpositions of cyclic type $\square\square$, eight rotations by $\pm 120^\circ$ about the lines a, b, c, d go to eight 3-cycles of cyclic type $\square\square\square$, and six rotations by 180° about the axes joining the midpoints of opposite edges go to six simple transpositions of cyclic type $\square\square$. The homomorphism $SO_{\text{cube}} \rightarrow S_3$ provided by the action of the group SO_{cube} on the lines x, y, z is compatible with both the isomorphism (12.9) and the surjection $S_4 \twoheadrightarrow S_3$ from Example 12.10. Its kernel consists of the Euclidean isometries of \mathbb{R}^3 sending each coordinate axis x, y, z to itself. Therefore, it coincides with the dihedral group D_2 . The isomorphism (12.9) identifies this dihedral group with the kernel of the surjection $S_4 \twoheadrightarrow S_3$ from Example 12.10.

Fig. 12.11 Cube on dodecahedron



Example 12.12 (Proper Dodecahedral Group and A_5) Each diagonal of a regular pentagonal face of a dodecahedron is uniquely completed by appropriate diagonals of the other faces¹⁶ to a cube whose edges are the chosen diagonals as in Fig. 12.11. There are altogether five such cubes on the surface of the dodecahedron. They are in bijection with the five diagonals of some fixed face of the dodecahedron. The proper group of the dodecahedron permutes these five cubes. This provides us with a homomorphism $\psi_{\text{dod}} : \text{SO}_{\text{dod}} \rightarrow S_5$. Looking at the model of the dodecahedron,¹⁷ it is easy to see that ψ_{dod} identifies $20 \cdot 3 = 60$ rotations of the dodecahedral group with 60 even permutations of five cubes as follows: $6 \cdot 4 = 24$ rotations by angles $2\pi k/5$, $1 \leq k \leq 4$, about the axes through the centers of opposite faces go to 24 maximal cycles of cyclic type $\square\square\square\square\square$; $10 \cdot 2 = 20$ rotations by angles $\pm 2\pi/3$ about the axes through the opposite vertices go to 20 3-cycles of cyclic type $\begin{smallmatrix} \square & \square \\ \square & \end{smallmatrix}$; 15 rotations by angles 180° about the axes through the midpoints of opposite edges go to 15 pairs of disjoint transpositions of cyclic type $\begin{smallmatrix} \square & \square \\ \square & \square \end{smallmatrix}$. Thus, we get an isomorphism $\psi_{\text{dod}} : \text{SO}_{\text{dod}} \cong A_5$.

Exercise 12.17 Prove independently that $\ker \psi_{\text{dod}} = \{\text{Id}\}$ and therefore ψ_{dod} is injective.

In contrast with Example 12.5, if we pass from the proper dodecahedral group to the complete one, then we do not get more permutations of cubes, because the central symmetry of the dodecahedron acts trivially on the cubes.

Exercise 12.18 Show that the groups S_5 and O_{dod} are not isomorphic.

¹⁶By taking exactly one diagonal in each face.

¹⁷I strongly recommend that you do [Exercise 12.10](#) before reading further.

12.5 Group Actions

12.5.1 Definitions and Terminology

Recall that we write $\text{Aut}(X)$ for the group of all bijections $X \simeq X$. For a group G and set X , a group homomorphism $\varphi : G \rightarrow \text{Aut}(X)$ is called an *action* of the group G on the set X or a *representation* of G by the transformations of X . We write $G : X$ if some action of G on X is given, and we write $\varphi_g : X \rightarrow X$ for the transformation $\varphi(g) : X \rightarrow X$ corresponding to $g \in G$ under the representation φ . The fact that the mapping $g \mapsto \varphi_g$ is a group homomorphism means that $\varphi_{gh} = \varphi_g \circ \varphi_h$ for all $g, h \in G$. When the action is clear from context or does not matter, we shall write simply gx instead of $\varphi_g(x)$. An action is called *transitive* if for every two points $x, y \in X$, there exists a transformation $g \in G$ such that $gx = y$. More generally, an action is called *m-transitive* if every ordered collection of m distinct points of X can be sent to any other such collection by some transformation from the group G . An action is called *free* if every element $g \neq e$ acts on X without fixed points, i.e., $\forall g \in G \forall x \in X \quad gx = x \Rightarrow g = e$. An action $\varphi : G \rightarrow \text{Aut} X$ is called *exact* (or *faithful*) if $\ker \varphi = e$, i.e., if every $g \neq e$ acts on X nonidentically. Every free action is clearly faithful. A faithful representation identifies a group G with some transformation group $\varphi(G) \subset \text{Aut}(X)$ of the set X . Usually, some geometric or algebraic structure on X respected by G stands behind such a representation.

Example 12.13 (Regular Actions) Let X be the set of all elements of a group G and $\text{Aut}(X)$ the group of set-theoretic bijections $X \simeq X$ knowing nothing about the group structure on G . The map

$$\lambda : G \rightarrow \text{Aut} X, \quad g \mapsto (\lambda_g : x \mapsto gx), \quad (12.10)$$

that sends $g \in G$ to the transformation¹⁸ of X provided by the left multiplication by g is an action of G on X , because $\lambda_{gh}(x) = ghx = \lambda_g(hx) = \lambda_g(\lambda_h(x)) = \lambda_g \circ \lambda_h(x)$. It is called the *left regular action* of G on itself. Since the equality $gh = h$ in G implies the equality $g = e$, the left regular action is free and therefore exact. Thus, every abstract group is isomorphic to some transformation group of an appropriate set. This remark is known as *Cayley's theorem*.

For example, the left regular representation realizes the additive group \mathbb{R} as the group of translations $\lambda_v : x \mapsto x + v$ of the real line. Similarly, the multiplicative group \mathbb{R}^* is realized as the group of homotheties $\lambda_c : x \mapsto cx$ of the punctured real line $\mathbb{R} \setminus \{0\}$.

Symmetrically, a *right regular action* $\varrho : G \rightarrow \text{Aut}(X)$ sends an element $g \in G$ to the right multiplication by g^{-1} , i.e., $\varrho_g : x \mapsto xg^{-1}$. We use g^{-1} in order to satisfy

¹⁸Note that this transformation of X is not a group homomorphism from G to G , because in general $g(h_1h_2) \neq (gh_1)(gh_2)$.

the condition $\varrho_{g_1 g_2} = \varrho_{g_1} \varrho_{g_2}$. The use of g would lead to an *antihomomorphism* $G \rightarrow \text{Aut}(X)$, which reverses the compositions.

Exercise 12.19 Verify that a right regular action is free.

Example 12.14 (Adjoint Action) The map $\text{Ad} : G \rightarrow \text{Aut}(G)$, $g \mapsto \text{Ad}_g$, sending $g \in G$ to the *conjugation-by- g automorphism*

$$\text{Ad}_g : G \rightarrow G, \quad h \mapsto ghg^{-1}, \quad (12.11)$$

is called the *adjoint action* of G on itself.

Exercise 12.20 Check that for each $g \in G$, the conjugation map (12.11) is an invertible *group homomorphism* from G to G . Then verify that the assignment

$$g \mapsto \text{Ad}_g$$

defines a group homomorphism from G to $\text{Aut } G$.

The image of the adjoint action is denoted by $\text{Int}(G) \stackrel{\text{def}}{=} \text{Ad}(G) \subset \text{Aut } G$ and is called the group of *inner* automorphisms of the group G . The elements of the complement $\text{Aut } G \setminus \text{Int}(G)$ are called *outer automorphisms* of G . In contrast with the regular actions, the adjoint action is neither free nor exact in general. For example, for an abelian group G , every inner automorphism (12.11) is the identity, and the adjoint action is trivial. For an arbitrary group G , the kernel of the adjoint action consists of all $g \in G$ such that $ghg^{-1} = h$ for all $h \in G$. The latter is equivalent to $gh = hg$ and means that g commutes with all elements of the group. Such elements g form a subgroup of G called the *center* of G and denoted by

$$Z(G) \stackrel{\text{def}}{=} \ker(\text{Ad}) = \{g \in G \mid \forall h \in G \ gh = hg\}. \quad (12.12)$$

The set of all elements $h \in G$ remaining fixed under the conjugation map (12.11) consists of all elements commuting with g . It is called the *centralizer* of g and denoted by

$$C_g \stackrel{\text{def}}{=} \{h \in G \mid hg = gh\}.$$

12.5.2 Orbits and Stabilizers

Every group G acting on a set X provides X with a binary relation $y \sim x$, meaning that $y = gx$ for some $g \in G$. This relation is reflexive, because $x = ex$. It is symmetric, because $y = gx \iff x = g^{-1}y$. It is transitive, because $y = gx$ and $z = hy$ force $z = (hg)x$. Therefore, we are dealing with an equivalence, which breaks X into a disjoint union of equivalence classes.¹⁹ The class of a point $x \in X$

¹⁹See Sect. 1.2 on p. 7.

consists of all points that can be obtained from x by means of transformations from G . It is denoted by $Gx = \{gx \mid g \in G\}$ and called the *orbit* of x under the action of G . The set of all orbits is denoted by X/G and called the *quotient* of X by the action of G . Associated with every orbit Gx is the *orbit map*,

$$\text{ev}_x : G \twoheadrightarrow Gx, \quad g \mapsto gx, \quad (12.13)$$

which is a kind of *evaluation*. The fiber of this map over a point $y \in Gx$ consists of all transformations sending x to y . It is called the *transporter* from x to y and is denoted by $G_{yx} = \{g \in G \mid gx = y\}$. The fiber over x consists of all transformations sending x to itself. It is called the *stabilizer* of x in G and is denoted by

$$\text{Stab}_G(x) = G_{xx} = \{g \in G \mid gx = x\}, \quad (12.14)$$

or just $\text{Stab}(x)$ when the reference to G is not important.

Exercise 12.21 Check that $\text{Stab}_G(x)$ is a subgroup of G .

Given $y = gx$ and $z = hx$, then for every $s \in \text{Stab}(x)$, the transformation hsg^{-1} is in G_{zy} . Conversely, if $fg = z$, then $h^{-1}fg \in \text{Stab}(x)$. Thus, there are two mutually inverse bijections

$$\begin{array}{ccc} \text{Stab}(x) & \xrightleftharpoons[h^{-1}fg \leftarrow f]{s \mapsto hsg^{-1}} & G_{zy} \end{array} \quad (12.15)$$

Hence, for any three points x, y, z lying in the same G -orbit, there is a bijection between the transporter G_{zy} and stabilizer $\text{Stab}(x)$. This simple remark leads to the following assertion.

Proposition 12.2 (Orbit Length Formula) *Let G be a finite transformation group of an arbitrary set and let x be any point of this set. Then*

$$|Gx| = |G| : |\text{Stab}_G(x)|.$$

In particular, the lengths of all orbits and orders of all stabilizers divide the order of the group.

Proof The group G decomposes into the disjoint union of the fibers of the surjective orbit map (12.13). All the fibers have cardinality $|\text{Stab}(x)|$. \square

Proposition 12.3 *The stabilizers of all points lying in the same orbit are conjugate:*

$$y = gx \Rightarrow \text{Stab}(y) = g \text{Stab}(x) g^{-1} = \{ghg^{-1} \mid h \in \text{Stab}(x)\}.$$

In particular, if one of them is finite, then they all are finite and have equal cardinalities.

Proof Take $z = y$ in the diagram (12.15). \square

Example 12.15 (Multinomial Coefficients Revisited) Fix an alphabet

$$A = \{a_1, a_2, \dots, a_k\}$$

of cardinality k and write X for the set of all words of length n in this alphabet. Equivalently, X can be viewed as the set of all maps $w : \{1, 2, \dots, n\} \rightarrow A$. Each permutation $\sigma \in S_n$ acts on X by $w \mapsto w\sigma^{-1}$. In terms of words, σ permutes the letters of a word by the rule $a_{w_1}a_{w_2} \dots a_{w_n} \mapsto a_{w_{\sigma^{-1}(1)}}a_{w_{\sigma^{-1}(2)}} \dots a_{w_{\sigma^{-1}(n)}}$.

Exercise 12.22 Check that this provides X with an action of S_n .

The S_n -orbit of a given word $w \in X$ consists of the words in which every letter $a_i \in A$ appears the same number of times as in w . Therefore, the points of the quotient X/S_n are naturally marked by the sequences m_1, m_2, \dots, m_k , where m_i is the number of occurrences of the letter a_i in each word of the orbit. The stabilizer $\text{Stab}(w)$ of a word w in such an orbit consists of $m_1! \cdot m_2! \dots m_k!$ independent permutations within the groups of coinciding letters. Therefore, the length of this orbit is

$$|S_n w| = \frac{|S_n|}{|\text{Stab}(w)|} = \frac{n!}{m_1! \cdot m_2! \dots m_k!} = \binom{n}{m_1 \dots m_k}$$

(compare with Example 1.2 on p. 5). We see that different orbits have different lengths, and the orders of stabilizers in different orbits are also different.

Exercise 12.23 For each Platonic solid Φ , consider the natural action of O_Φ on the set of (a) faces, (b) edges, (c) vertices of Φ . Calculate $|O_\Phi|$ by means of Proposition 12.2 applied to each of these actions.

Example 12.16 (Conjugation Classes in the Symmetric Group) The orbits of the adjoint action $\text{Ad} : G \rightarrow \text{Aut}(G)$ are called *conjugation classes* in G . Such a class $\text{Ad}(G)h = \{ghg^{-1} \mid g \in G\}$ consists of all elements conjugate to a given element $h \in G$. Let us describe the conjugation classes in the symmetric group S_n . For a permutation $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n) \in S_n$, its conjugate permutation $g\sigma g^{-1}$ sends the element $g(i)$ to the element $g(\sigma_i)$ for each $i = 1, 2, \dots, n$. Therefore, the conjugation map $\text{Ad}_g : \tau \mapsto g\tau g^{-1}$ provided by $g = (g_1, g_2, \dots, g_n) \in S_n$ sends a cycle $|i_1, i_2, \dots, i_k| \in S_n$ to the cycle $|g_{i_1}, g_{i_2}, \dots, g_{i_k}|$ formed by the g -images of the elements from the original cycle. If $\sigma \in S_n$ has cyclic type λ and disjoint cycles of σ are written in the rows of the diagram λ , then the action of Ad_g just permutes the numbers in the cells of the diagram λ by the rule $i \mapsto g_i$. Therefore, the conjugation classes in S_n are in bijection with the Young diagrams λ of weight²⁰ $|\lambda| = n$. The adjoint orbit corresponding to the diagram λ consists of all permutations obtained as follows: fill the cells of λ by the numbers $1, 2, \dots, n$ without repetitions and form the product of cycles recorded in the rows of diagram. The adjoint action of an

²⁰That is, consisting of n cells.

element $g \in S_n$ on such an orbit just permutes the numbers in the cells of the diagram as prescribed by g . Such a permutation centralizes the product of cycles if and only if it cyclically permutes the elements within the rows or arbitrarily permutes the rows of equal length in their entirety. Thus, the centralizer has order

$$z_\lambda \stackrel{\text{def}}{=} 1^{m_1} \cdot m_1! \cdot 2^{m_2} \cdot m_2! \cdots n^{m_n} \cdot m_n! = \prod_{\alpha=1}^n m_\alpha! \alpha^{m_\alpha},$$

where $m_i = m_i(\lambda)$ is the number of rows with length i in λ . The cardinality of the conjugation class of a permutation of cyclic type λ is equal to $n!/z_\lambda$. For example, the permutation

$$\sigma = (6, 5, 4, 7, 2, 1, 9, 8, 3) \in S_9$$

can be decomposed into disjoint cycles as $|7, 9, 3, 4| |2, 5| |1, 6| |8|$ and corresponds to the filled Young diagram

| | | | |
|---|---|---|---|
| 7 | 9 | 3 | 4 |
| 2 | 5 | | |
| 1 | 6 | | |
| 8 | | | |

Its centralizer is isomorphic to $\mathbb{Z}/(4) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2)$, where the factors are generated by the cyclic shifts within the first three rows and the transposition of the second and third rows. It has cardinality 32. The conjugation class of g consists of $9!/32 = 11340$ permutations.

12.5.3 Enumeration of Orbits

Given an action of a finite group G on a finite set X , the computation of the total number of orbits, that is, the cardinality of X/G , is met by an obvious difficulty: since orbits have different lengths, we have to use separate enumeration procedures for orbits of different types and, by the way, enumerate these types. The following claim avoids this problem quite elegantly.

Theorem 12.2 (Burnside–Pólya–Redfield Formula) *Let a finite group G act on a finite set X . For each $g \in G$, let X^g be the fixed-point set of the transformation g , i.e., $X^g = \{x \in X \mid gx = x\} = \{x \in X \mid g \in \text{Stab}(x)\}$. Then $|X/G| = |G|^{-1} \sum_{g \in G} |X^g|$.*

Proof Write $F \subset G \times X$ for the set of all pairs (g, x) such that $gx = x$. The projections $F \rightarrow X$ and $F \rightarrow G$ show that

$$\bigsqcup_{x \in X} \text{Stab}(x) = F = \bigsqcup_{g \in G} X^g.$$

The second equality leads to $|F| = \sum_{g \in G} |X^g|$. The first equality implies that $|F| = |G| \cdot |X/G|$, because the stabilizers of all points in any orbit Gx have the same cardinality $|G|/|Gx|$, and the sum of these cardinalities equals $|G|$. \square

Example 12.17 (Necklaces) Given an unrestricted supply of uniform beads of n distinct colors, how many different necklaces can be made using six beads? The answer is given by the number of orbits in the natural action of the dihedral group D_6 on the set of colorings of the dihedral vertices in n given colors. The group D_6 consists of 12 transformations: the identity e , two rotations $\tau^{\pm 1}$ by angles $\pm 60^\circ$, two rotations $\tau^{\pm 2}$ by angles $\pm 120^\circ$, the central symmetry τ^3 , three reflections $\sigma_{14}, \sigma_{23}, \sigma_{36}$ in the main diagonals, and three reflections $\bar{\sigma}_{14}, \bar{\sigma}_{23}, \bar{\sigma}_{36}$ in the perpendicular bisectors of the sides. The identity fixes all n^6 colorings. The colorings fixed by the other transformations are shown in Fig. 12.12. Taking there all possible combinations of colors, we get n, n^2, n^3, n^4 , and n^3 colorings respectively. Thus, by Theorem 12.2, the number of six-bead necklaces equals $(n^6 + 3n^4 + 4n^3 + 2n^2 + 2n)/12$.

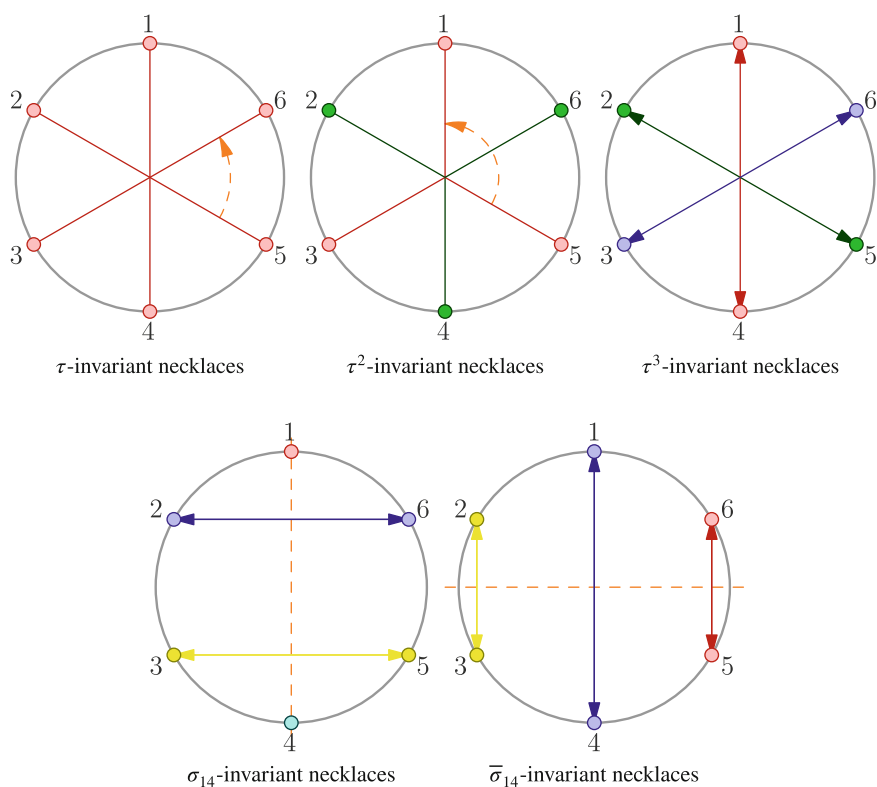


Fig. 12.12 Symmetric necklaces from six beads

12.6 Factorization of Groups

12.6.1 Cosets

Each subgroup $H \subset G$ provides G with two equivalence relations coming from the left and right regular actions of H on G . The left regular action $\lambda_h : g \mapsto hg$ leads to the equivalence $g_1 \sim_L g_2$, meaning that $g_1 = hg_2$ for some $h \in H$. It decomposes G into the disjoint union of orbits $Hg \stackrel{\text{def}}{=} \{hg \mid h \in H\}$, called *right cosets* of H in G . The set of all right cosets of H is denoted by $H \backslash G$.

Exercise 12.24 Check that the following conditions on a subgroup $H \subset G$ and elements $g_1, g_2 \in G$ are equivalent: **(a)** $Hg_1 = Hg_2$, **(b)** $g_1g_2^{-1} \in H$, **(c)** $g_2g_1^{-1} \in H$.

The right regular action $\varrho_h : g \mapsto gh^{-1}$ leads to the equivalence $g_1 \sim_R g_2$, meaning that $g_1 = g_2h$ for some $h \in H$. It decomposes G into a disjoint union of orbits $gH \stackrel{\text{def}}{=} \{gh \mid h \in H\}$ called *left cosets*²¹ of H in G . The set of all left cosets of H is denoted by G/H .

Since both left and right regular actions of H on G are free, all orbits in both actions have length $|H|$. Therefore, each of the two actions produces $|G|/|H|$ orbits. This number is called the *index* of the subgroup H in the group G and is denoted by $[G : H] \stackrel{\text{def}}{=} |G/H|$. As a byproduct, we get the following theorem of Lagrange.

Theorem 12.3 (Lagrange's Theorem) *The order of a finite group G is divisible by the order of every subgroup $H \subset G$.* \square

Corollary 12.3 *The order of each element of a finite group divides the order of the group.*

Proof The order of an element g is equal to the order of the cyclic subgroup $\langle g \rangle$ spanned by g . \square

12.6.2 Normal Subgroups

A subgroup $H \subset G$ is called *normal*²² if all inner automorphisms of G map H to itself, i.e., $gHg^{-1} = H$ for all $g \in G$. We write $H \triangleleft G$ for a normal subgroup H .

Exercise 12.25 Assume that $gHg^{-1} \subset H$ for all $g \in G$. Show that $H \triangleleft G$.

The equality $gHg^{-1} = H$ is equivalent to the equality $gH = Hg$. Therefore, $H \triangleleft G$ if and only if the left cosets of H coincide with the right: $gH = Hg$ for all $g \in G$.

Example 12.18 (Kernels of Homomorphisms) In Proposition 12.1 on p. 289, we proved that $g(\ker \varphi) = (\ker \varphi)g$ for every group homomorphism $\varphi : G_1 \rightarrow G_2$

²¹Or *left shifts*.

²²Or *invariant*.

and $g \in G_1$. Hence, $\ker \varphi \triangleleft G_1$ is normal in G_1 . This can be seen as well from [Exercise 12.25](#): for every $h \in \ker \varphi$ and $g \in G$, we have

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e.$$

Hence $g \ker(\varphi) g^{-1} \subset \ker \varphi$ for all $g \in G$.

Example 12.19 ($V_4 \triangleleft S_4$) The Klein four group $V_4 \subset S_4$ formed by the identity permutation and three permutations of cyclic type $\begin{smallmatrix} \square & \square \\ \square & \square \end{smallmatrix}$ is normal, because it is the union of two conjugation classes in S_4 . At the same time, V_4 is the kernel of the epimorphism $S_4 \twoheadrightarrow S_3$ from [Example 12.10](#) on p. 291.

Example 12.20 (Inner Automorphisms) The inner automorphisms of a group G form a normal subgroup $\text{Int}(G) \triangleleft \text{Aut}(G)$, because for an inner automorphism $\text{Ad}_g : h \mapsto ghg^{-1}$ and an arbitrary automorphism $\varphi : G \xrightarrow{\sim} G$, the conjugate automorphism $\varphi \circ \text{Ad}_g \circ \varphi^{-1} = \text{Ad}_{\varphi(g)}$ is inner.

Exercise 12.26 Check the latter equality.

Example 12.21 (Affine Group) Recall²³ that associated with every vector space V is the group of affine automorphisms $\text{Aff}(V)$ of the affine space $\mathbb{A}(V)$ over V . It follows from [Proposition 6.6](#) and [Proposition 6.7](#) on p. 148 that the differentiation map

$$D : \text{Aff}(V) \rightarrow \text{GL}(V), \quad \varphi \mapsto D\varphi, \quad (12.16)$$

which takes an affine map to its differential, is a group homomorphism. By [Proposition 6.7](#), its kernel coincides with the subgroup of shift transformations $\tau_v : p \mapsto p + v$. Thus, the parallel shifts form a normal subgroup of $\text{Aff}(V)$. This subgroup is isomorphic to the additive group of the vector space V .

Exercise 12.27 Verify that $\varphi \tau_v \varphi^{-1} = \tau_{D\varphi(v)}$ for every $v \in V$ and $\varphi \in \text{Aff}(V)$.

Note that the differentiation map ([12.16](#)) is surjective, because for every $F \in \text{GL}(V)$ and $p \in \mathbb{A}(V)$, the map $F_p : \mathbb{A}(V) \rightarrow \mathbb{A}(W)$, $q \mapsto p + F(\overrightarrow{pq})$, is affine, bijective, and has $D_{F_p} = F$.

12.6.3 Quotient Groups

Given a group G and a subgroup $H \subset G$, an attempt to define a group structure on the set of left cosets G/H by means of our usual formula

$$(g_1H) \cdot (g_2H) \stackrel{\text{def}}{=} (g_1g_2)H \quad (12.17)$$

²³See [Sect. 6.5.6](#) on p. 148.

fails, because equal cosets $g_1H = f_1H$ and $g_2H = f_2H$ may produce $(g_1g_2)H \neq (f_1f_2)H$.

Exercise 12.28 Let $G = S_3$ and $H = \langle s_{12} \rangle$, where $s_{12} = (2, 1, 3)$. Explicitly indicate some cosets for which definition (12.17) is incorrect.

Proposition 12.4 *The group structure on G/H is well defined by (12.17) if and only if $H \triangleleft G$.*

Proof Let formula (12.17) provide G/H with a well-defined binary operation. Then this operation is associative, because $(g_1H \cdot g_2H) \cdot g_3H = (g_1g_2)H \cdot g_3H = ((g_1g_2)g_3)H = (g_1(g_2g_3))H = g_1H \cdot (g_2g_3)H = g_1H \cdot (g_2H \cdot g_3H)$. It has the unit $eH = H$. Every coset gH has an inverse coset $g^{-1}H$. Hence G/H is a group, and the quotient map $G \twoheadrightarrow G/H$, $g \mapsto gH$, is a group homomorphism with kernel H . Therefore, $H \triangleleft G$ by Example 12.18.

Conversely, let $H \triangleleft G$ be normal. For subsets $A, B \in G$, we put

$$AB \stackrel{\text{def}}{=} \{ab \mid a \in A, b \in B\}.$$

For example, $HH = H$. This notation agrees with the notation gH for the left coset, because the latter consists of all gh with $h \in H$. Since the product $(g_1H)(g_2H) = \{ab \mid a \in g_1H, b \in g_2H\}$ depends only on the cosets, it is enough to check that $(g_1H)(g_2H) = g_1g_2H$. This forces the latter coset to be independent of the choice of $g_1 \in g_1H$, $g_2 \in g_2H$. Since H is normal, $gH = Hg$ for all $g \in G$. We use this twice for $g = g_1$ and $g = g_1g_2$ to get $(g_1H)(g_2H) = Hg_1g_2H = g_1g_2HH = g_1g_2H$, as required. \square

Definition 12.2 (Quotient Group) For a normal subgroup $H \triangleleft G$, the set of cosets G/H equipped with the group structure

$$g_1H \cdot g_2H \stackrel{\text{def}}{=} \{sr \mid s \in g_1H, r \in g_2H\} = (g_1g_2)H$$

is called the *quotient* (or *factor*) group of G by H . The map $G \twoheadrightarrow G/H$, $g \mapsto gH$, is called a *quotient homomorphism*.

Corollary 12.4 (Decomposition of Homomorphisms) *A group homomorphism $\varphi : G_1 \rightarrow G_2$ can be factored as the composition of a quotient epimorphism*

$$G_1 \twoheadrightarrow G_1 / \ker \varphi$$

followed by an injective homomorphism

$$G_1 / \ker \varphi \hookrightarrow G_2$$

sending the coset $g \ker \varphi \in G_1 / \ker \varphi$ to $\varphi(g) \in G_2$. In particular, $\text{im } \varphi \simeq G / \ker \varphi$.

Proof The corollary states that $\varphi^{-1}(\varphi(g)) = g \ker \varphi$ for every $\varphi(g) \in \text{im } \varphi$. We have already seen this in Proposition 12.1 on p. 289. \square

Proposition 12.5 For two subgroups $N, H \subset G$ such that $N \triangleleft G$, the product $HN \stackrel{\text{def}}{=} \{hx \mid h \in H, x \in N\}$ is a subgroup of G . Moreover, $H \cap N \triangleleft H$, $N \triangleleft HN$, and $HN/N \simeq H/(H \cap N)$.

Proof The product $HN \subset G$ is a subgroup, because for all $h_1, h_2, h \in H$ and all $x_1, x_2, x \in N$, we have

$$\begin{aligned} h_1 x_1 h_2 x_2 &= (h_1 h_2) (h_2^{-1} x_1 h_2 \cdot x_2) \in HN, \\ (hx)^{-1} x^{-1} h^{-1} &= h^{-1} (h x h^{-1}) \in HN, \end{aligned} \tag{12.18}$$

since $h_2^{-1} x_1 h_2 \in N$ and $h x h^{-1} \in N$. The subgroup $H \cap N \triangleleft H$ is normal, because $N \triangleleft G$ is normal. Now consider the surjective map $\varphi : HN \rightarrow H/(H \cap N)$ sending the product hx to the coset $h \cdot (H \cap N)$. It is well defined, because the equality $h_1 x_1 = h_2 x_2$ implies that $h_1^{-1} h_2 = x_1 x_2^{-1} \in H \cap N$, and therefore $h_1 \cdot (H \cap N) = h_1 \cdot (h_1^{-1} h_2) \cdot (H \cap N) = h_2 \cdot (H \cap N)$. It follows from (12.18) that φ is a group homomorphism. Since $\ker \varphi = eN = N$, we conclude that $H/(H \cap N) = \text{im } \varphi \simeq HN/\ker \varphi = HN/N$ by Corollary 12.4. \square

Exercise 12.29 Let $\varphi : G_1 \twoheadrightarrow G_2$ be a surjective group homomorphism. Show that for every normal subgroup $N_2 \triangleleft G_2$, its preimage $N_1 = \varphi^{-1}(N_2)$ is normal in G_1 , and $G_1/N_1 \simeq G_2/N_2$.

Problems for Independent Solution to Chap. 12

Problem 12.1 Show that an associative binary operation $G \times G \rightarrow G$ provides G with a group structure if and only if for all $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in G$.

Problem 12.2 Enumerate all the subgroups in the dihedral groups²⁴ D_4 and D_6 .

Problem 12.3 Show that every subgroup of a cyclic group is cyclic.

Problem 12.4 Find the parity of the order of an arbitrary odd permutation.

Problem 12.5 In the permutation group S_5 , calculate (a) g^{100} for $g = (3, 5, 4, 1, 2)$, (b) the number of elements remaining fixed under conjugation by the permutation $(3, 5, 1, 2, 4)$.

Problem 12.6 (Involutive Permutations) A permutation σ is called *involutive* if $\sigma^2 = \text{Id}$. Prove that σ is involutive if and only if the Young diagram depicting the cyclic type of σ has at most two columns. Show that every cycle of length ≥ 3 in S_n is a composition of two involutive permutations.

²⁴See Example 12.4 on p. 284.

Problem 12.7 (N. N. Konstantinov) The residents of town N may exchange their houses. However, only simple two-way exchanges²⁵ are allowed, and each homeowner can make at most one exchange per day. Can an arbitrary complex exchange be made in two days?

Problem 12.8 Is it possible to swap the “1 and “2” tiles in the 15-puzzle following the game of fifteen rules? (All the other tiles should return to their initial positions.)²⁶

Problem 12.9 (Orders of Elements) For an arbitrary group:

- (a) Show that every element of odd order is the square of some element of the group.
- (b) Find $\text{ord}(fg)$ if $\text{ord}(gf) = n$.
- (c) Prove that $\text{ord}(g^n) = \text{ord}(g)/\text{GCD}(n, \text{ord}(g))$ for all $n \in \mathbb{N}$.
- (d) For $fg = gf$, prove that $\text{ord}(fg) \mid \text{LCM}(\text{ord}(f), \text{ord}(g))$.

Problem 12.10 Let $\text{ord}(g) = 2$ for all $g \neq e$ in some group G . Show that G is abelian and describe all such finite groups.

Problem 12.11 Let finite groups G, H for each $k \in \mathbb{N}$ have the same number of order- k elements. Is it true that $G \simeq H$? For the continuation of this story, see [Problem 14.27](#) on p. 359.

Problem 12.12 We say that a group G is spanned by a set $B \subset G$ if every element of G is a finite composition of elements of B (possibly repeated). (a) Is S_n spanned by the transpositions $|1, 2\rangle$ and cycle $|1, 2, 3, \dots, n\rangle$? (b) Is A_n spanned by cycles $|1, 2, 3\rangle, |1, 2, 4\rangle, \dots, |1, 2, n\rangle$?

Problem 12.13 Show that every finite group spanned by two nontrivial involutions²⁷ is isomorphic to a dihedral group.

Problem 12.14 Find the orders of the complete and proper groups of the standard (a) n -cube,²⁸ (b) n -cocube,²⁹ (c) n -simplex.³⁰ To begin with, consider $n = 4$.

Problem 12.15 (Group Q_8) Let us equip the set $Q_8 \stackrel{\text{def}}{=} \{\pm e, \pm i, \pm j, \pm k\}$ with a multiplication such that e is a neutral element, signs are multiplied by the standard rules,³¹ $i^2 = j^2 = k^2 = -e$, and $ij = -ji = k, jk = -kj = i, ki = -ik = j$. Check that this is a group structure and find out whether Q_8 is isomorphic to D_4 .

²⁵Such that A takes B 's and B takes A 's house; any more complicated combination (e.g., A takes B 's house, B takes C 's house, and C takes A 's house) is forbidden.

²⁶See https://en.wikipedia.org/wiki/15_puzzle.

²⁷That is, elements $\sigma \neq e$ such that $\sigma^2 = e$.

²⁸See [Problem 10.7](#) on p. 248.

²⁹See [Problem 10.13](#) on p. 250.

³⁰See [Problem 10.9](#) on p. 249.

³¹As in \mathbb{R} : $+\cdot+ = -\cdot- = +, +\cdot- = -\cdot+ = -$.

Problem 12.16 (Direct Product of Groups) For a set of groups $\{G_x\}_{x \in X}$, verify that their set-theoretic direct product $\prod_{x \in X} G_x$ equipped with componentwise composition

$$(g_x)_{x \in X} (h_x)_{x \in X} \stackrel{\text{def}}{=} (g_x h_x)_{x \in X}$$

is a group. Given two subgroups $F, H \subset G$, show that $G \simeq F \times G$ if and only if the following three conditions hold simultaneously:

$$(1) F \cap H = \{e\}, \quad (2) FH = G, \quad (3) \forall f \in F \forall h \in H, \quad fh = hf.$$

Problem 12.17 For which $n, m \in \mathbb{N}$ do we have $D_{mn} \simeq D_m \times \mathbb{Z}/(n)$?

Problem 12.18 Find all pairs of isomorphic groups in the following collections of groups:

(a) $D_8, D_4 \times \mathbb{Z}/(2), Q_8 \times \mathbb{Z}/(2)$;

(b) $S_4, D_{12}, D_6 \times \mathbb{Z}/(2), D_3 \times \mathbb{Z}/(2) \times \mathbb{Z}/(2), D_3 \times \mathbb{Z}/(4), Q_8 \times \mathbb{Z}/(3), D_4 \times \mathbb{Z}/(3)$.

Problem 12.19 List all Platonic solids³² Φ such that $O_\Phi \simeq SO_\Phi \times \mathbb{Z}/(2)$.

Problem 12.20 For each platonic solid Φ , find the lengths of all the orbits for the tautological actions of the groups O_Φ and SO_Φ on Φ . Indicate all points whose orbits are shorter than a generic orbit.

Problem 12.21 (Diagonal Actions) Let a group G act on sets X_1, X_2, \dots, X_m and define the *diagonal action* of G on $X_1 \times X_2 \times \dots \times X_m$ by

$$g : (x_1, x_2, \dots, x_m) \mapsto (gx_1, gx_2, \dots, gx_m).$$

Write V (respectively E) for the set of vertices (respectively edges) of the standard cube in \mathbb{R}^3 . The proper group of the cube SO_{cube} acts tautologically on V and E . Describe the orbits of the diagonal action of SO_{cube} on (a) $V \times V$, (b) $V \times E$, (c) $E \times E \times E$.

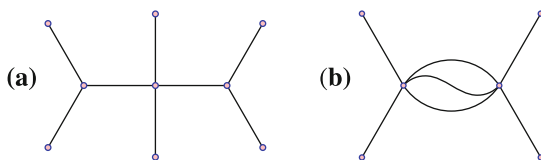
Problem 12.22 For the standard action of the permutation group S_n on $X = \{1, 2, \dots, n\}$, describe the orbits of the diagonal action of S_n on X^m for all $n \geq m$. (To begin with, take $m = 2, 3, \dots$)

Problem 12.23 A finite group acts transitively on a set of cardinality at least 2. Show that there is some element in the group acting without fixed points.

Problem 12.24 Given an unrestricted supply of uniform beads of n distinct colors, how many different necklaces can be made from (a) four, (b) seven, (c) eight, (d) nine beads?

³²See Exercise 12.10 on p. 283.

Problem 12.25 Given an unrestricted supply of uniform pieces of string of n distinct colors, how many distinct³³ string linkage patterns of the form



can be made from them? (The pieces of string are tied together at the endpoints only.)

Problem 12.26 Find the index of the subgroup $\text{Int}(A_5)$ in $\text{Aut}(A_5)$.

Problem 12.27* Find an outer automorphism³⁴ of S_6 .

Problem 12.28 The product of two left cosets³⁵ of a subgroup H is always a left coset of H . Show that H is normal.

Problem 12.29 Show that for every pair of normal subgroups N, H with $N \cap H = \{e\}$, we have $nh = hn$ for all $n \in N, h \in H$.

Problem 12.30 Is there a nonabelian group G such that every subgroup of G is normal?

Problem 12.31 (Commutator Subgroup) The smallest subgroup of G containing all *commutators* $[g, h] \stackrel{\text{def}}{=} ghg^{-1}h^{-1}$, $g, h \in G$, is called the *commutator subgroup* of G and is denoted by $[G, G]$. Show that (a) $[G, G] \triangleleft G$ is normal and the quotient group $G/[G, G]$ is abelian. (b) $[G, G]$ is contained in the kernel of every homomorphism from G to an arbitrary abelian group.

Problem 12.32 Find the order $|\text{PSL}_2(\mathbb{F}_q)|$.

Problem 12.33 Construct isomorphisms of the following groups:

- (a) $\text{PSL}_2(\mathbb{F}_3) \cong A_4$,
- (b) $\text{PGL}_2(\mathbb{F}_4) \cong A_5$,
- (c) $\text{PSL}_2(\mathbb{F}_5) \cong A_5$,
- (d) $\text{PSL}_3(\mathbb{F}_2) \cong \text{PSL}_2(\mathbb{F}_7)$,
- (e) $\text{PSL}_2(\mathbb{F}_9) \cong A_6$.

Problem 12.34 (Steiner Systems and Mathieu Groups) A collection S of subsets of cardinality k in a finite set X of cardinality n is called a *Steiner system* $S(t, k, n)$

³³That is, nonsuperposable in \mathbb{R}^3 .

³⁴

Hint: Find two different conjugation classes of equal cardinalities and try to map one to the other by an appropriate group homomorphism.

³⁵That is, the set of all products xy , where x and y run through two left cosets.

if every subset of cardinality t in X is contained in exactly one set from the collection S . For such a collection S , the group

$$\text{Aut } S \stackrel{\text{def}}{=} \{g \in \text{Aut}(X) \mid \forall Y \in S \ g(Y) \in S\}$$

is called the *automorphism group* of S .

- (a) Given a Steiner system $S(t, k, n)$, construct the Steiner system $S(t-1, k-1, n-1)$.
- (b) Use the projective geometry over the finite field \mathbb{F}_q to construct the Steiner systems $S(2, q, q^2)$ and $S(2, q+1, q^2+q+1)$ for all $q = p^k$ with prime $p \in \mathbb{N}$.
- (c) Show that the Steiner system $S(5, 6, 12)$ for

$$X = \mathbb{P}_1(\mathbb{F}_{11}) = \{[0], [1], \dots, [10], \infty\}$$

is formed by the $\text{PGL}_2(\mathbb{F}_{11})$ -orbits of all squares $[0], [1], [4], [9], [3], [5]$ in \mathbb{F}_{11} .

(d*) Construct the Steiner system $S(5, 8, 24)$.

(e*) Find the orders of the *Mathieu groups*³⁶

$$M_{10} \stackrel{\text{def}}{=} \text{Aut } S(3, 4, 10),$$

$$M_{22} \stackrel{\text{def}}{=} \text{Aut } S(3, 6, 22),$$

$$M_{11} \stackrel{\text{def}}{=} \text{Aut } S(4, 5, 11),$$

$$M_{23} \stackrel{\text{def}}{=} \text{Aut } S(4, 7, 23),$$

$$M_{12} \stackrel{\text{def}}{=} \text{Aut } S(5, 6, 12),$$

$$M_{24} \stackrel{\text{def}}{=} \text{Aut } S(5, 8, 24).$$

- (f) Show that the Mathieu groups M_{11}, M_{22}, M_{23} appear as stabilizers of some points under the tautological actions of the Mathieu groups M_{12}, M_{23}, M_{24} on their Steiner systems.
- (g) Construct an isomorphism $\text{PGL}_3(\mathbb{F}_4) \simeq M_{21} \stackrel{\text{def}}{=} \text{Aut } S(2, 5, 21)$.
- (h*) Construct an isomorphism $A_6 \simeq [M_{10}, M_{10}]$.

Chapter 13

Descriptions of Groups

13.1 Generators and Relations

13.1.1 Free Groups

Associated with a set X is the *free group* F_X spanned by X and described as follows. Consider an alphabet formed by letters x and x^{-1} , where $x \in X$. On the set of all words¹ of this alphabet consider the smallest equivalence relation “=” that identifies two words obtained from each other by inserting or deleting any number of copies of xx^{-1} or $x^{-1}x$ (or both) at the beginning, or at the end, or between any two sequential letters. By definition, the elements of the free group F_X are the equivalence classes of words with respect to this equivalence. The composition is the concatenation of words: $x_1x_2 \dots x_k \cdot y_1y_2 \dots y_m \stackrel{\text{def}}{=} x_1x_2 \dots x_ky_1y_2 \dots y_m$.

Exercise 13.1 Verify that composition is well defined on the equivalence classes.

The class of the empty word is the unit of F_X . Inversion swaps the letters x, x^{-1} and reverses the order of the letters: $(x_1x_2 \dots x_m)^{-1} = x_m^{-1} \dots x_2^{-1}x_1^{-1}$. We say that a word is *irreducible* if it does not contain any fragments xx^{-1} or $x^{-1}x$.

Exercise 13.2 Check that there is exactly one irreducible word in each equivalence class and that it is the shortest word of the class.

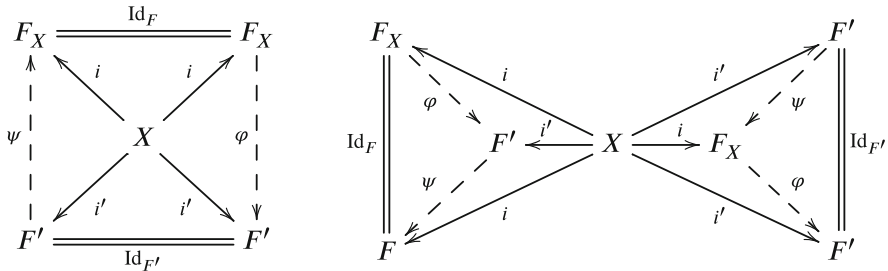
The elements of X are called the *generators* of the free group F_X . The free group with k generators is denoted by F_k . The group $F_1 \simeq \mathbb{Z}$ is the cyclic group of infinite order. The group F_2 is formed by classes of words written with four letters x, y, x^{-1}, y^{-1} . It is already quite vast.

Exercise 13.3 Construct an injective group homomorphism $F_{\mathbb{N}} \hookrightarrow F_2$.

¹Including the empty word \emptyset .

Proposition 13.1 (Universal Property of Free Groups) *The map $i : X \rightarrow F_X$ that sends $x \in X$ to the class of the word x possesses the following universal property: for every group G and every map of sets $\Gamma : X \rightarrow G$, there exists a unique group homomorphism $\text{ev}_\Gamma : F_X \rightarrow G$ such that $\Gamma = \text{ev}_\Gamma \circ i$. It takes the class of the word $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m}$, where $x_v \in X$ and $\varepsilon_v = \pm 1$, to the product $\Gamma(x_1)^{\varepsilon_1} \Gamma(x_2)^{\varepsilon_2} \dots \Gamma(x_m)^{\varepsilon_m} \in G$. If some group F' and some map $i' : X \rightarrow F'$ also have this universal property, then there exists a unique group isomorphism $\varphi : F_X \xrightarrow{\sim} F'$ such that $i' = \varphi \circ i$.*

Proof The homomorphism ev_Γ is unique, because it has to act by the rule described in the proposition. At the same time, this rule certainly produces a well-defined homomorphism $\text{ev}_\Gamma : F_X \rightarrow G$ such that $\Gamma = \text{ev}_\Gamma \circ i$. Thus, the map $i : X \rightarrow F_X$ has the required universal property. Let $i' : X \rightarrow F'$ be another map such that for every map $\Gamma : X \rightarrow G$, there exists a unique homomorphism $\text{ev}'_\Gamma : F' \rightarrow G$ extending Γ . Then there are unique homomorphisms $\varphi = \text{ev}'_{i'} : F_X \rightarrow F'$ and $\psi = \text{ev}_i : F' \rightarrow F_X$ that can be fitted into the commutative diagrams



The second diagram shows that $i = \psi \varphi \circ i$ and $i' = \varphi \psi \circ i'$. These equalities imply that $\psi \varphi = \text{Id}_{F_X}$ and $\psi = \text{Id}_{F'}$, because the factorizations $i = \text{ev}_i \circ i$, $i' = \text{ev}'_{i'} \circ i'$ hold for unique $\text{ev}_i : F_X \rightarrow F_X$, $\text{ev}'_{i'} : F' \rightarrow F'$, and we know that $\text{ev}_i = \text{Id}_{F_X}$ and $\text{ev}'_{i'} = \text{Id}_{F'}$ produce for such factorizations. \square

13.1.2 Presentation of a Group by Generators and Relators

Let G be an arbitrary group and X any set allowing an injective map to G . By Proposition 13.1, every inclusion $\Gamma : X \hookrightarrow G$ can be uniquely extended to a homomorphism $\text{ev}_\Gamma : F_X \rightarrow G$, $x \mapsto \Gamma(x)$. If ev_Γ is surjective, then the subset $\Gamma(X) \subset G$ is called a *generating set* for G , and the elements $g_x = \Gamma(x) \in G$, indexed by $x \in X$, are called *generators* of the group G . In this case, G is exhausted by finite products of the form $g_1^{\varepsilon_1} g_2^{\varepsilon_2} \dots g_k^{\varepsilon_k}$, where $g_i \in \Gamma(X)$ and $\varepsilon_i = \pm 1$. A group G is called *finitely generated* if it admits a finite generating set. For an inclusion $\Gamma : X \hookrightarrow G$ that produces the surjective homomorphism

$$\text{ev}_\Gamma : F_X \twoheadrightarrow G, \quad (13.1)$$

the kernel $\ker \text{ev}_\Gamma \triangleleft F_X$ is called the *group of relations* among the generators $g_x = \Gamma(x)$. The subset $R \subset \ker \text{ev}_\Gamma$ is called a *relating set*, and its elements are called *relators*, if $\ker \text{ev}_\Gamma$ is the minimal normal subgroup in F_X containing R with respect to inclusions.² This means that every relation $w \in \ker \text{ev}_\Gamma$ can be assembled from some finite collection of words in R by means of a finite number of compositions, inversions, and conjugations by arbitrary elements of F_X . In other words, each relator $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m} \in R$ produces the identity $g_{x_1}^{\varepsilon_1} g_{x_2}^{\varepsilon_2} \cdots g_{x_m}^{\varepsilon_m} = e$ in G , and all constraints on the generators g_x in G can be deduced from these identities by multiplying two identities side by side, reversing both sides of an identity, and multiplying both sides of an identity by an element of G from either the left or the right.

Every group G can be generated by some $\Gamma(X) \subset G$, at worst for $X = G$. If some epimorphism (13.1) is given and some relating set $R \subset F_X$ is known, then the pair (X, R) is called a *presentation* of G by generators and relators. Every presentation determines the group G uniquely up to isomorphism, because

$$G \simeq F_X/N_R,$$

where $N_R \triangleleft F_X$ is the smallest normal subgroup containing R . A group G is called *finitely presented* if it admits a presentation (X, R) where both sets X, R are finite. A happy choice of presentation (e.g., with small X, R and nice relators) sometimes can appreciably clarify the structure of a group or its action somewhere. However, in general, the description of a group by generators and relators may be quite obscure. Even elucidation as to whether the group is trivial may be extremely difficult. In the formal sense accepted in mathematical logic, the latter problem is *undecidable* even in the class of finitely presented groups.³

Proposition 13.2 *Let a group G be generated by elements $\{g_x\}_{x \in X}$ with relating set $R \subset F_X$. Then for every group H and every family of elements $\{h_x\}_{x \in X} \subset H$, there exists at most one homomorphism $\psi : G \rightarrow H$ such that $\psi(g_x) = h_x$ for all $x \in X$. It exists if and only if for every relator $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m} \in R$, the equality $h_{x_1}^{\varepsilon_1} h_{x_2}^{\varepsilon_2} \cdots h_{x_m}^{\varepsilon_m} = e$ holds in H . In this case, ψ is well defined by*

$$\psi(g_{x_1}^{\varepsilon_1} g_{x_2}^{\varepsilon_2} \cdots g_{x_m}^{\varepsilon_m}) = h_{x_1}^{\varepsilon_1} h_{x_2}^{\varepsilon_2} \cdots h_{x_m}^{\varepsilon_m}. \quad (13.2)$$

Proof The family $\{h_x\}_{x \in X} \subset H$ is the same as the map $\Phi : X \rightarrow H, x \mapsto h_x$. By Proposition 13.1, such maps are in bijection with the group homomorphisms $\text{ev}_\Phi : F_X \rightarrow H$. Such a homomorphism is factorized through the quotient group $G = F_X/N_R$ as

$$\begin{array}{ccc} F_X & \xrightarrow{\text{ev}_\Phi} & H \\ & \searrow & \nearrow \psi \\ & G & \end{array}$$

²That is, the intersection of all normal subgroups containing R .

³This is a part of the famous *undecidability of the word problem* proved by Pyotr Novikov in 1955.

if and only if $N_R \subset \ker \text{ev}_\Phi$. Since $N_R \triangleleft F_X$ is the smallest normal subgroup containing R and $\ker \text{ev}_\Phi \triangleleft F_X$ is normal, the inclusion $N_R \subset \ker \text{ev}_\Phi$ is equivalent to the inclusion $R \subset \ker \text{ev}_\Phi$. If it holds, then by Proposition 13.1, the homomorphism ψ has to be defined by formula (13.2). \square

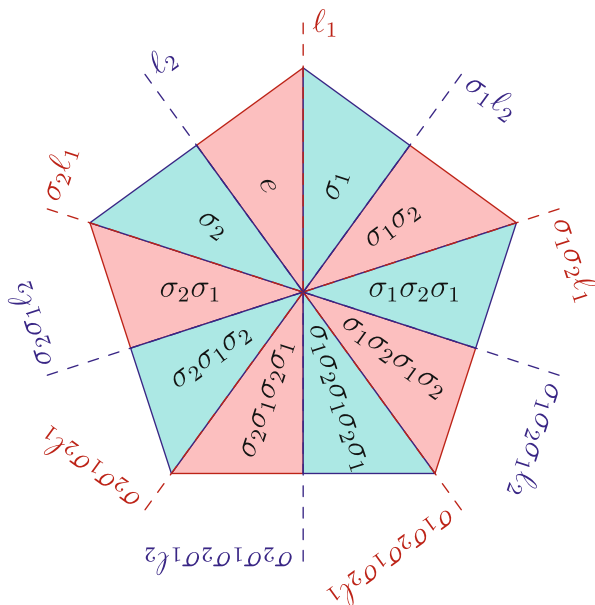
13.1.3 Presentations for the Dihedral Groups

Let us show that the dihedral group D_n can be presented by the generating set $X = \{x_1, x_2\}$ and relating set $R = \{x_1^2, x_2^2, (x_1 x_2)^n\}$, that is, it can be generated by two elements $\sigma_1, \sigma_2 \in D_n$ such that

$$\sigma_1^2 = \sigma_2^2 = (\sigma_1 \sigma_2)^n = e \quad (13.3)$$

and all the relations between σ_1 and σ_2 follow from (13.3). The reflection lines cut the regular n -gon into $2n$ right triangles (see Fig. 13.1).

Fig. 13.1 Reflections generating the dihedral group



Choose one of them and label it $e \in D_n$. Since every isometry of the plane is uniquely determined by its action on this triangle, $2n$ transformations $g \in D_n$ are in bijection with our $2n$ triangles. Let us label triangle $g(e)$ by g . Write ℓ_1, ℓ_2 for the reflection lines that pass through the sides of triangle e , and let $\sigma_1, \sigma_2 \in D_n$ be the reflections in these lines. Then the triangles obtained from e by sequential counterclockwise reflections in the sides become labeled $\sigma_2, \sigma_2 \sigma_1,$

$\sigma_2\sigma_1\sigma_2, \sigma_2\sigma_1\sigma_2\sigma_1, \dots$ and the triangles obtained by clockwise reflections become labeled by $\sigma_1, \sigma_1\sigma_2, \sigma_1\sigma_2\sigma_1, \sigma_1\sigma_2\sigma_1\sigma_2, \dots$

Exercise 13.4 Let $\sigma_\ell : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be reflection in the line ℓ . Check that for every isometry $F : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, we have $F \circ \sigma_\ell \circ F^{-1} = \sigma_{F(\ell)}$, or equivalently, $\sigma_{F(\ell)} \circ F = F \circ \sigma_\ell$.

The composition $\sigma_1 \circ \sigma_2$ is a rotation in the direction from ℓ_2 to ℓ_1 by the doubled angle between ℓ_2 and ℓ_1 , which equals $2\pi/n$ for D_n . Therefore, $\sigma_1^2 = \sigma_2^2 = (\sigma_1\sigma_2)^n = e$. By Proposition 13.2, the assignment $x_1 \mapsto \sigma_1, x_2 \mapsto \sigma_2$ gives a well-defined epimorphism $\text{ev}_{\sigma_1, \sigma_2} : F_2/N_R \twoheadrightarrow D_n$, where $N_R \triangleleft F_2$ is the smallest normal subgroup containing $R = \{x_1^2, x_2^2, (x_1x_2)^n\}$. It remains to verify that it is injective, that is, that two words from F_2 sent to the same $g \in D_n$ are always congruent modulo R . Each word constructed from the alphabet $\{x_1, x_2\}$ is congruent modulo R to a word of length at most $2n - 1$ looking either like $x_1x_2x_1 \dots$ or like $x_2x_1x_2 \dots$. We have seen above that all words of the first type are sent by $\text{ev}_{\sigma_1, \sigma_2}$ to different elements of D_n , labeling different triangles. The same is true for all words of the second type. Two words of different types go to the same element of D_n if and only if the corresponding words $\sigma_1\sigma_2\sigma_1 \dots$ and $\sigma_2\sigma_1\sigma_2 \dots$ label the same triangle g in Fig. 13.1, that is, if they encode two different ways of rolling triangle e into g : either counterclockwise or clockwise. In this case, the coincidence is written as $\text{ev}_{\sigma_1, \sigma_2}(\underbrace{x_1x_2x_1 \dots}_k) = \text{ev}_{\sigma_1, \sigma_2}(\underbrace{x_2x_1x_2 \dots}_{2n-k})$. But the relation $\underbrace{x_1x_2x_1 \dots}_k = \underbrace{x_2x_1x_2 \dots}_{2n-k}$ certainly follows from the relations $x_1^2 = x_2^2 = (x_1x_2)^n = e$.

Exercise 13.5 Check this.

13.1.4 Presentations of the Groups of Platonic Solids

Let Φ be one of the Platonic solids with triangular faces, that is, the tetrahedron, octahedron, or icosahedron. Let us put

$m_1 =$ the number of faces meeting at each vertex of Φ ,

$m_2 =$ the number of faces meeting at each edge of $\Phi = 2$,

$m_3 = 3$.

The reflection planes of Φ produce the *barycentric subdivision* of each face into six right triangles,⁴ $2m_1$ of which meet at the vertices of Φ , $2m_2$ at the midpoints of the edges of Φ , and $2m_3$ at the centers of that faces of Φ . The total number of triangles equals $N = 6 \cdot (\text{number of faces})$. Let us collect these combinatorial data in a table:

| Φ | m_1 | m_2 | m_3 | N |
|-------------|-------|-------|-------|-----|
| tetrahedron | 3 | 3 | 2 | 24 |
| octahedron | 4 | 3 | 2 | 48 |
| icosahedron | 5 | 3 | 2 | 120 |

Note that a regular n -gon could be included in this table with values $m_1 = 2$, $m_2 = 2$, $m_3 = n$, $N = 4n$ if we agree that it has two faces exchanged by reflection in the plane of the n -gon.

The intersections of the mirror planes of Φ with its circumscribed sphere triangulate this sphere by N congruent triangles with angles π/m_1 , π/m_2 , π/m_3 equal to the angles between the reflection planes of Φ . In the tetrahedral case, the stereographic projection of this triangulation onto a plane can be seen in Fig. 13.2 on p. 315. Let us label one triangle of the triangulation with $e \in O_\Phi$ and write π_1 , π_2 , π_3 for the reflection planes that cut it out. We number the planes in such a way that the angle between π_i and π_j equals π/m_k . Since every isometry of \mathbb{R}^3 sending Φ to itself preserves the center of Φ , such an isometry is uniquely determined by its action on the triangle e . Therefore, the transformations $g \in O_\Phi$ are in bijection with the triangles⁵ of the triangulation. Let us label triangle $g(e)$ with the element $g \in O_\Phi$. Then every transformation $h \in O_\Phi$ sends each triangle g to the triangle hg . Write $\sigma_i \in O_\Phi$, $i = 1, 2, 3$, for the reflections in the planes π_i . The composition $\sigma_i \circ \sigma_j$ is a rotation about the line $\pi_i \cap \pi_j$ in the direction from π_j to π_i by the angle $2\pi/m_k$, the doubled angle between π_i and π_j . Therefore, the reflections σ_i satisfy the six relations

$$\sigma_i^2 = e \quad \text{and} \quad (\sigma_i \sigma_j)^{m_k} = e, \quad (13.4)$$

where $i = 1, 2, 3$ and (i, j, k) runs through three cyclic permutations of $(1, 2, 3)$.

⁴With vertices at the barycenter of the face, at the barycenters of its edges, and at its vertices.

⁵Note that we get a new explanation for the identity $|O_\Phi| = N = 6 \cdot (\text{number of faces})$.

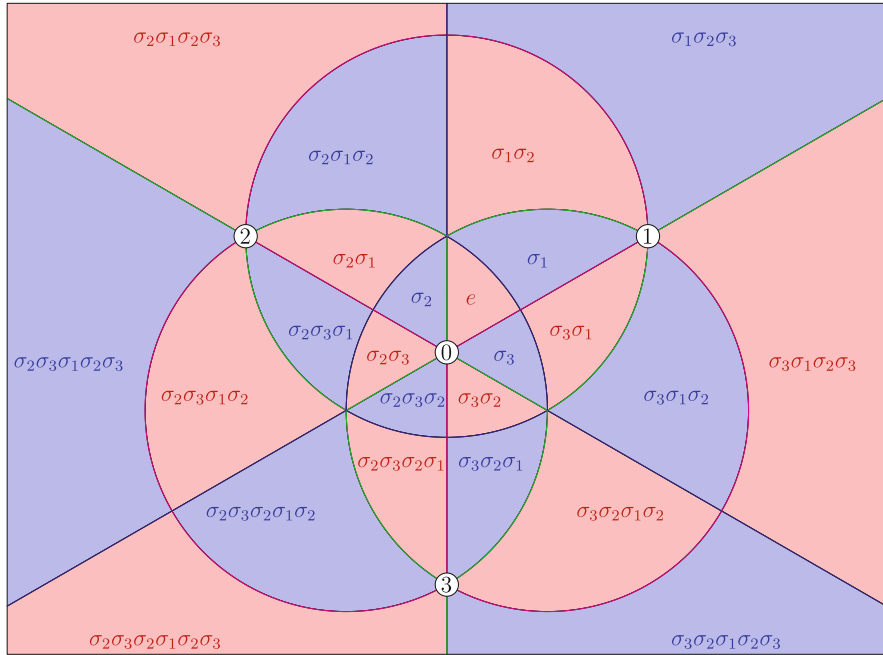


Fig. 13.2 Triangulation of the sphere by the reflection planes of the tetrahedron $[0, 1, 2, 3]$ (stereographic projection from the point opposite vertex $[0, 1, 2, 3]$ onto the equatorial plane parallel to the face $[1, 2, 3]$)

Proposition 13.3 *The complete group O_Φ of a Platonic solid Φ with triangular faces is presented by generators $\{x_1, x_2, x_3\}$ and relators*

$$x_i^2 \quad \text{and} \quad (x_i x_j)^{m_k}. \quad (13.5)$$

Proof The previous discussion shows that the evaluation $x_i \mapsto \sigma_i$ produces a well-defined homomorphism $\varphi : F_3/N \rightarrow O_\Phi$, where $N \triangleleft F_3$ is the smallest normal subgroup containing the six words (13.5). It takes the class of the word $w = x_{i_1} x_{i_2} \dots x_{i_m}$, where $i_v \in \{1, 2, 3\}$, to

$$g = \varphi(w) = \sigma_{i_1} \sigma_{i_2} \dots \sigma_{i_m} \in O_\Phi.$$

When we read the sequence of reflection $\sigma_{i_1} \sigma_{i_2} \dots \sigma_{i_m}$ from left to right,⁶ the triangles labeled by elements

$$g_v \stackrel{\text{def}}{=} \sigma_{i_1} \sigma_{i_2} \dots \sigma_{i_v} \quad (13.6)$$

⁶That is, in the opposite order to that in which the reflections are made.

form a continuous ribbon g_0, g_1, \dots, g_m , which starts at $g_0 = e$ and ends at $g_m = g$. Every triangle g_v of this ribbon is obtained from the preceding triangle g_{v-1} by reflection in the plane $g_{v-1}(\pi_{i_v})$. Under the superposition of triangle e with triangle g_{v-1} provided by the transformation g_{v-1} , this reflection plane matches the side of e that is cut out by π_{i_v} . Indeed, by [Exercise 13.4](#) on p. 313, reflection in the plane $g_{v-1}(\pi_{i_v})$ coincides with the composition $g_{v-1}\sigma_{i_v}g_{v-1}^{-1} \in O_\Phi$, which maps triangle g_{v-1} to triangle $g_{v-1}\sigma_{i_v}g_{v-1}^{-1}g_{v-1} = g_{v-1}\sigma_{i_v} = g_v$.

Therefore, if we label the sides of triangle e by 1, 2, 3 in accordance with the numbers of planes that cut them out of the sphere and then extend this marking to all triangles in such a way that congruent sides receive identical labels, then the reflection $g_{v-1} \mapsto g_v$ is made through the i_v th side, whose mark $i_v \in \{1, 2, 3\}$ equals the v th index i_v in the sequence (13.6).

Thus, to write a sequence of numbers $i_1, i_2, \dots, i_m \in \{0, 1, 2\}$ producing a ribbon of triangles (13.6) that goes from e to any prescribed triangle g , we proceed as follows. Connect some internal points of triangles e, g by a smooth curve⁷ that does not pass through the vertices of the triangulation and crosses all sides transversally. Then go along this curve from e to g and write down the labels on the sequential edges that we cross. We obtain thereby a sequence of labels $i_{v_1}i_{v_2} \dots i_{v_m}$ such that $g = \sigma_{i_1}\sigma_{i_2} \dots \sigma_{i_m} = \varphi(x_{i_1}x_{i_2} \dots x_{i_m})$. Figure 13.3 shows how this works. Red, green, and yellow are used there instead of labels 1, 2, 3 respectively. In particular, we see that $\varphi : F_3/N \rightarrow O_\Phi$ is surjective. Let us check now that it is injective, i.e., any two words w_1, w_2 from the alphabet $\{x_1, x_2, x_3\}$ mapped to the same transformation $g \in O_\Phi$ are equivalent modulo relators (13.5). Each of these words produces a ribbon of triangles beginning at e and ending at g . In these ribbons, the v th triangle is obtained from the preceding, $(v-1)$ th, triangle by reflection in the side marked by the same index $i_v \in \{1, 2, 3\}$ as the v th letter x_{i_v} in the corresponding word w_1 or w_2 . Let us draw a smooth curve as above within each of the two ribbons and deform the second curve into the first across the surface of the sphere in such a way that at each moment, the deformed curve remains transversal to all the sides it crosses. Each time the curve meets some vertex v common to $2m_k$ triangles, the ribbon of triangles that corresponds to the curve is changed as follows. A sequence of ℓ sequential triangles covering a part of the regular m_k -gon centered at v is replaced by the complementary sequence of $2m_k - \ell$ triangles covering the remaining part of the m_k -gon and proceeding around v in the opposite direction. On the side of the words, this corresponds to replacement of some ℓ -letter fragment looking like $x_i x_j x_i x_j x_i \dots$ by a $(2m_k - \ell)$ -letter fragment looking like $x_j x_i x_j x_i x_j \dots$. Since these two fragments are equal modulo relations $x_i^2 = x_j^2 = (x_i x_j)^{m_k} = e$, the class of the word in F_3/N_R remains unchanged. \square

⁷For instance by a *geodesic* cut out of the sphere by a plane passing through the center of the sphere.

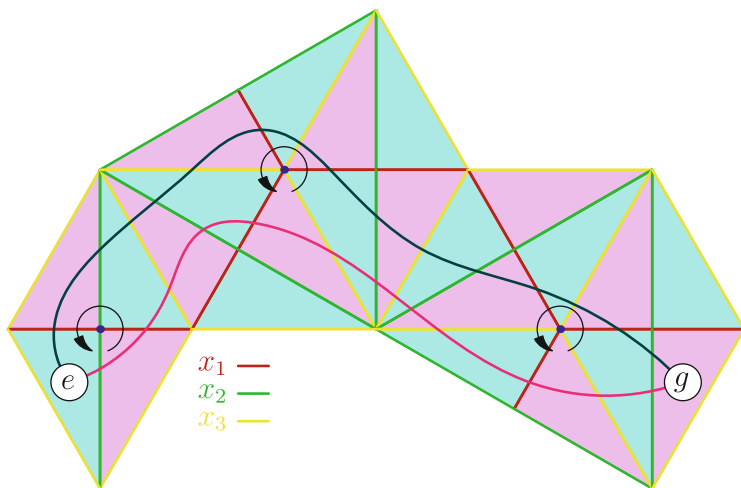


Fig. 13.3 $x_1x_2x_3x_2x_3x_1x_3x_1x_2x_3x_2x_1x_3x_1x_2 = g = x_2x_1x_3x_2x_1x_3x_2x_3x_2x_3x_1x_3x_2$

For example, the upper and lower trajectories leading from e to g in Fig. 13.3 produce the words

$$x_1x_2x_3x_2x_3x_1x_3x_1x_2x_3x_2x_1x_3x_1x_2$$

and

$$x_2x_1x_3x_2x_1x_3x_2x_3x_2x_3x_1x_3x_2$$

transformed into each other by means of the cyclic relations

$$x_1x_2 = x_2x_1, \quad x_3x_1x_3x_1 = x_1x_3, \quad x_3x_1x_3 = x_1x_3x_1$$

applied at labeled vertices.

Exercise 13.6 Chose an internal point a in triangle e and some point b not opposite to a within triangle g such that the shortest of the two geodesics⁸ joining a and b does not pass through the vertices of the triangulation.⁹ Use this geodesic to write a word $w \in F_3$ such that $\varphi(w) = g$ as above. Show that the length of this word does not depend on the agreed-upon choice of points and that g cannot be represented by a shorter word.

⁸That is, arcs of a great circle cut out of the sphere by the plane passing through a , b , and the center of sphere.

⁹This always can be achieved by a small perturbation of b , because there are finitely many geodesics passing through a and some vertex of the triangulation.

13.2 Presentation of the Symmetric Group

Consider the symmetric group $S_{n+1} = \text{Aut}\{0, 1, \dots, n\}$ and write $\sigma_i = |(i-1), i\rangle$ for the transposition of sequential elements $(i-1), i$, where $1 \leq i \leq n$.

Exercise 13.7 Check that transpositions σ_i generate S_{n+1} and satisfy the relations

$$\sigma_i^2 = e, \quad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \quad \sigma_i \sigma_j = \sigma_j \sigma_i \text{ for } |i-j| \geq 2.$$

Thus, we have a surjective group homomorphism

$$\varphi : F_n/N \twoheadrightarrow S_{n+1}, \quad x_i \mapsto \sigma_i, \quad (13.7)$$

where $N \triangleleft F_n$ is the smallest normal subgroup containing the words

$$x_i^2, \quad (x_i x_{i+1})^3 \quad \text{and} \quad (x_i x_j)^2 \text{ for } |i-j| \geq 2. \quad (13.8)$$

Below we will give two proofs that φ is injective. The geometric approach from Sect. 13.2.1 will repeat the arguments used in the proof of Proposition 13.3 for the tetrahedral case, but instead of the tetrahedron, the standard n -simplex in \mathbb{R}^{n+1} will be considered. In Sect. 13.2.2, geometric arguments will be translated into combinatorial language for the sake of those who prefer a pedantic transfer of letters from one side of an equation to the other rather than imagining n -dimensional pictures.

13.2.1 Complete Group of a Regular Simplex

Write \mathbb{A}^n for \mathbb{R}^n sitting within \mathbb{R}^{n+1} as an affine hyperplane drawn through the heads of all standard basis vectors¹⁰ $e_0, e_1, \dots, e_n \in \mathbb{R}^{n+1}$. The convex hull of the points $e_0, e_1, \dots, e_n \in \mathbb{A}^n$ is called the *standard n -simplex*¹¹ and denoted by Δ . This is a regular polyhedron with center $c = ((n+1)^{-1}, (n+1)^{-1}, \dots, (n+1)^{-1})$. We vectorize the affine space \mathbb{A}^n using c as the origin. To prevent many-storied indices, we denote the vertices of Δ just by numbers $i \in \{0, 1, \dots, n\}$. For $n = 3$, the simplex Δ is the regular tetrahedron $[0, 1, 2, 3] \subset \mathbb{R}^3$ considered in Sect. 13.1.4.

Exercise 13.8 Given two ordered collections of $(n+1)$ points in \mathbb{A}^n such that no hyperplane whatever contains any of them, prove that there exists a unique

¹⁰Equivalently, the hyperplane $\mathbb{A}^n \subset \mathbb{R}^{n+1}$ is given by the equation $x_0 + x_1 + \dots + x_n = 1$.

¹¹See Problem 10.9 on p. 249.

affine map¹² $\mathbb{A}^n \rightarrow \mathbb{A}^n$ sending one collection to the other. Show that this map is automatically invertible.

The exercise implies that elements of the complete group O_Δ are in a natural bijection with the permutations of vertices $[0, 1, \dots, n]$. If $g \in S_{n+1}$ is such a permutation, we use the same letter g to denote the linear isometry $\Delta \xrightarrow{\sim} \Delta$ sending vertex i to vertex $g_i = g(i)$ for all i .

The simplex Δ has $n(n+1)/2$ reflection hyperplanes π_{ij} passing through the midpoint of edge $[i, j]$ and the opposite face of codimension 2, the convex hull of vertices $\{0, 1, \dots, n\} \setminus \{i, j\}$. The transposition σ_{ij} of vertices i, j is exactly the reflection in the hyperplane π_{ij} .

Exercise 13.9 Check that the hyperplanes π_{ij} and π_{km} are orthogonal for $\{i, j\} \cap \{k, m\} = \emptyset$ and $\angle(\pi_{ij}, \pi_{jk}) = \pi/3$ for $i \neq k$.

The hyperplanes π_{ij} decompose the simplex Δ into $n!$ simplices forming the *barycentric subdivision* of Δ . All these simplices have a common vertex at the center of Δ . Their other vertices fall into the barycenters of the faces of Δ . The faces of Δ are numbered by subsets in $\{0, 1, \dots, n\}$. Let $[i_0, i_1, \dots, i_m] \subset \Delta$ be the m -dimensional face formed by the convex hull of vertices $\{i_0, i_1, \dots, i_m\}$. We denote its barycenter by $c_{\{i_0, i_1, \dots, i_m\}}$. In particular, one-point subsets $\{i\}$ correspond to the vertices $c_{\{i\}} = i$ of Δ , whereas the whole set $\{0, 1, \dots, n\}$ gives the center $c_{\{0, 1, \dots, n\}} = c$ of Δ itself. Associated with every permutation $g = (g_0, g_1, \dots, g_n) \in S_{n+1}$ is the n -simplex $\Delta_g \subset \Delta$ with vertices at the barycenters $c_{\{g_0\}}, c_{\{g_0, g_1\}}, c_{\{g_0, g_1, g_2\}}, \dots, c_{\{g_0, g_1, \dots, g_n\}}$, the first of which is vertex g_0 of Δ , the second is the midpoint of the edge $[g_0, g_1]$ outgoing from g_0 , the third is the center of the triangular face $[g_0, g_1, g_2]$ attached to the edge $[g_0, g_1]$, etc. All simplices Δ_g are distinct, and every transformation $g \in O_\Delta$ maps each Δ_h to Δ_{gh} . Thus, all simplices of the barycentric subdivision of Δ are bijectively marked by permutations $g \in S_{n+1}$, or equivalently, by orthogonal transformations $g : \Delta \xrightarrow{\sim} \Delta$ superposing the beginning simplex $\Delta_e = [c_{\{0\}}, c_{\{0,1\}}, c_{\{0,1,2\}}, \dots, c_{\{0,1,\dots,n-1\}}, c_{\{0,1,\dots,n\}}]$ with simplices Δ_g . For each g , we project the $(n-1)$ -dimensional face of Δ_g opposite vertex c from c onto the sphere $S^{n-1} \subset \mathbb{A}^n$ circumscribed about Δ . Let us label the resulting spherical $(n-1)$ -simplices by g . We get a triangulation of the circumscribed sphere by $n!$ congruent spherical simplices marked by transformations $g \in O_\Delta$ in such a way that the transformation g maps the spherical simplex h to the spherical simplex gh exactly as took place in Sect. 13.1.4.

For $n = 3$, which corresponds to the group S_4 , we get the triangulation of the sphere S^2 by 24 congruent triangles with angles of $\pi/3, \pi/3, \pi/2$ shown in Fig. 13.2 on p. 315. In higher dimensions, the picture is completely similar.

The beginning simplex e is cut out of the sphere by n hyperplanes $\pi_i \stackrel{\text{def}}{=} \pi_{i-1,i}$, for $1 \leq i \leq n$. By Exercise 13.9, they intersect at dihedral angles $\angle(\pi_i, \pi_{i+1}) = 60^\circ$ and $\angle(\pi_i, \pi_j) = 90^\circ$ for $|i - j| \geq 2$. Write σ_i for the reflection in π_i (note that

¹²See Sect. 6.5.5 on p. 148.

this agrees with notation from Sect. 13.2). The compositions $\sigma_i\sigma_{i+1}$ and $\sigma_i\sigma_j$, where $|j - i| \geq 2$, act identically on the $(n - 2)$ -dimensional intersections $\pi_i \cap \pi_{i+1}$, $\pi_i \cap \pi_j$. In the perpendicular 2-planes, they act as rotations by angles 120° and 180° respectively. Therefore, $\sigma_1, \sigma_2, \dots, \sigma_n$, satisfy the relations $\sigma_i^2 = (\sigma_i\sigma_j)^2 = (\sigma_i\sigma_{i+1})^3 = e$ for all $1 \leq i, j \leq n$ such that $|i - j| \geq 2$.

We conclude that there is a well-defined homomorphism

$$\varphi : F_n/N \rightarrow O_\Delta, x_i \mapsto \sigma_i,$$

where $N \triangleleft F_n$ is the smallest normal subgroup containing the words (13.8). The word $w = x_{i_1}x_{i_2} \dots x_{i_m} \in F_n$ produces a chain g_0, g_1, \dots, g_m of spherical simplices

$$g_v \stackrel{\text{def}}{=} \sigma_{i_1}\sigma_{i_2} \dots \sigma_{i_v}$$

with $g_0 = e$ and $g_m = \varphi(w)$. In this chain, each simplex g_v is the reflection of the preceding simplex g_{v-1} in the face $g_{v-1}(\pi_{i_v})$, which matches the i_v th face¹³ of the beginning simplex e under the superposition of e with g_{v-1} provided by the transformation $g_{v-1} \in O_\Delta$. To write the word w such that $\varphi(w) = g$, we join some internal points of simplices e, g by a smooth curve transversally crossing all codimension-1 faces that it meets at interior points of these faces. Then we walk from e to g along the curve and write the numbers i_1, i_2, \dots, i_m of the sequential codimension-1 faces we cross. Clearly, $g = \varphi(x_{i_1}x_{i_2} \dots x_{i_m})$.

Any two words in F_3 representing the same element $g \in O_\Delta$ are obtained in the way just described from some curves going from e to g . We can deform one of these curves into the other within S^{n-1} in such a way that all the time, it remains transversal to all codimension-1 walls that it meets. Consider a moment when the curve is moved over the wall crossing the locus of codimension 2. Such a locus is congruent to some intersection $\pi_i \cap \pi_j \cap S^{n-1}$. If we project S^{n-1} along $\pi_i \cap \pi_j$ onto the 2-dimensional Euclidean plane perpendicular to $\pi_i \cap \pi_j$, then in a neighborhood of the point to which $\pi_i \cap \pi_j$ is projected we see a picture like that in Fig. 13.3 on p. 317. Therefore, if $\angle(\pi_i, \pi_j) = 90^\circ$, then the passage through $\pi_i \cap \pi_j \cap S^{n-1}$ replaces some fragment $x_i x_j$ by the reversed fragment $x_j x_i$. Two words obtained from each other by such a replacement are equivalent in F_3/N , because of the relation $(x_i x_j)^2 = e$. If $\angle(\pi_i, \pi_j) = 60^\circ$, then $j = i + 1$ and all possible mutations of the word agree with the relation $(x_i x_{i+1})^3 = e$. We conclude that two words mapped by φ to the same g are always equivalent modulo the relations (13.8), i.e.,

$$\varphi : F_n/N \simeq S_{n+1}$$

is an isomorphism.

¹³Which is cut out of the sphere by the reflection plane π_{i_v} .

Exercise 13.10 Choose some internal points a, b in the spherical simplices e, g such that b is not opposite to a and the short geodesic¹⁴ joining a and b crosses walls of codimension 1 at internal points of the faces of the spherical simplices. Use this geodesic to write a word $w \in F_3$ such that $\varphi(w) = g$. Show that the length of this word does not depend on the agreed-upon choice of a, b and that g cannot be represented by a shorter word.

13.2.2 Bruhat Order

Recall¹⁵ that $I(g)$ for $g \in S_{n+1}$ means the *inversion number* of g , that is, the total number of ordered pairs (i, j) such that $0 \leq i < j \leq n$ and $g(i) > g(j)$. We are going to show that $I(g)$ is the minimal length of the expression $g = \sigma_{i_1} \cdot \sigma_{i_2} \cdots \sigma_{i_m}$, where $i_v \in \{1, 2, \dots, n\}$ and σ_i denotes the transposition of sequential elements $(i-1, i)$ as before. For this reason, $I(g)$ is also called the *length* of the permutation g .

Exercise 13.11 Verify that $0 \leq I(g) \leq n(n+1)/2$ in S_{n+1} and the only permutations with inversion numbers 0 and $n(n+1)/2$ are respectively

$$\text{Id} = (0, 1, \dots, n) \quad \text{and} \quad \delta \stackrel{\text{def}}{=} (n, (n-1), \dots, 1, 0).$$

For every $g \in S_{n+1}$ and $i = 1, 2, \dots, n$, the permutation $g\sigma_i$ is constructed from g by swapping the $(i-1)$ th symbol $g(i-1)$ with the i th symbol $g(i)$:

$$\begin{aligned} & (g(1), \dots, g(i-2), \mathbf{g(i-1)}, \mathbf{g(i)}, g(i+1), \dots, g(n)) \circ \sigma_i \\ &= (g(1), \dots, g(i-2), \mathbf{g(i)}, \mathbf{g(i-1)}, g(i+1), \dots, g(n)). \end{aligned}$$

Thus, $I(g\sigma_i) = I(g) + 1$ for $g(i-1) < g(i)$ and $I(g\sigma_i) = I(g) - 1$ for $g(i-1) > g(i)$. Since right multiplication by σ_i can increase $I(g)$ by at most 1, every decomposition $g = \sigma_{i_1} \cdot \sigma_{i_2} \cdots \sigma_{i_m}$ has length $m \geq I(g)$.

Exercise 13.12 Check that if $I(h) > 0$, then there exist sequential elements $i, i+1$ such that $h(i-1) > h(i)$, and for this i , the equality $I(h\sigma_i) = I(h) - 1$ holds.

The exercise implies that there exists a chain of right multiplications by appropriate σ_i that kill some inversion pair of *sequential* elements in each step. Such a chain is forced to reduce g down to e in exactly $I(g)$ steps:

$$g \mapsto g\sigma_{i_1} \mapsto g\sigma_{i_1}\sigma_{i_2} \mapsto \cdots \mapsto g\sigma_{i_1}\sigma_{i_2} \cdots \sigma_{i_{I(g)}} = e.$$

¹⁴That is, the shortest of two arcs of the great circle cut out of $S^{n-1} \subset \mathbb{A}^n$ by the 2-dimensional plane passing through a, b , and the center of sphere.

¹⁵See Sect. 9.2 on p. 208.

Therefore, $g = \sigma_{i_{l(g)}} \sigma_{i_{l(g)-1}} \cdots \sigma_{i_1}$. This proves once more the surjectivity of the homomorphism (13.7) and shows that $I(g)$ coincides with the minimal length of words mapped to g by (13.7).

Every word $w \in F_n$ of length $I(g)$ such that $\varphi(w) = g$ is called a *minimal word* for g . The decomposition $g = \varphi(w) = \sigma_{i_1} \cdot \sigma_{i_2} \cdots \sigma_{i_{l(g)}}$ obtained from (any) minimal word $w = x_{i_1} \cdot x_{i_2} \cdots x_{i_{l(g)}}$ for g is called a *shortest decomposition* of g . Note that both are not unique in general.

Let us write $g < h$ if $h = g\sigma_{i_1} \cdot \sigma_{i_2} \cdots \sigma_{i_k}$, where $k > 0$, and

$$I(g\sigma_{i_1} \cdot \sigma_{i_2} \cdots \sigma_{i_v}) = I(g\sigma_{i_1} \cdot \sigma_{i_2} \cdots \sigma_{i_{v-1}}) + 1$$

for all $v = 1, 2, \dots, k$, i.e., each multiplication by the next σ_{i_v} swaps some noninverse pair of sequential elements. The binary relation $g \leq h$, meaning that either $g = h$ or $g < h$, provides S_{n+1} with a partial order¹⁶ called the *Bruhat order*.

Exercise 13.13 Convince yourself that the binary relation $g \leq h$ is reflexive, skew-symmetric, and transitive.

For every shortest decomposition $g = \sigma_{i_1} \cdot \sigma_{i_2} \cdots \sigma_{i_{l(g)}}$, the initial segments

$$g_v = \sigma_{i_1} \sigma_{i_2} \cdots \sigma_{i_v}$$

form a strictly increasing sequence with respect to the Bruhat order. It begins with $g_0 = e$, ends with $g_m = g$, and each g_v is obtained from g_{v-1} by the transposition of some noninverse pair of sequential elements $g_{v-1}(i_{v-1}) < g_{v-1}(i_v)$. The injectivity of $\varphi : F_n/N \rightarrow S_{n+1}$ follows from the next claim.

Proposition 13.4 *Every word $w \in F_n$ is equivalent to some minimal word for the permutation $\varphi(w) \in S_{n+1}$ modulo the relations $x_i^2 = e$, $x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$, and $x_i x_j = x_j x_i$ for $|i - j| \geq 2$. Any two minimal words for $\varphi(w)$ are also equivalent.*

Proof Write $\ell(w)$ for the length of the word w and use induction on $\ell(w)$. For $\ell(w) = 0$, i.e., $w = \emptyset$, the statement is trivial. Assume that it has been proved for all words w of length $\ell(w) \leq m$. It is enough to verify the statement for every word $w x_v$ such that $\ell(w) \leq m$. Let $g = \varphi(w)$. Then $\varphi(w x_v) = g\sigma_v$. If w is not minimal for g , then by the induction hypothesis, w is equivalent to some shorter word. Therefore, the word $w x_v$ is also equivalent to some shorter word u . By the induction hypothesis, u is equivalent to some minimal word for $\varphi(u) = g\sigma_v$, and all minimal words for $g\sigma_v$ are equivalent to each other. Thus, the statement is true in this case.

Now assume that w is minimal for g . There are two possibilities: either $g(v-1) > g(v)$ or $g(v-1) < g(v)$. In the first case, g has a minimal word of the form $u x_v$, which is equivalent to w by the induction hypothesis. Then $w x_v \sim u x_v x_v \sim u$, where \sim means equivalence of words modulo $N \triangleleft F_n$. Therefore, the permutation $\varphi(w x_v) = \varphi(u)$ is represented by a word u equivalent to $w x_v$ that is strictly shorter

¹⁶See Sect. 1.4 on p. 13.

than wx_v . Applying the induction hypothesis to u , we conclude that u is equivalent to some minimal word for $\varphi(wx_v)$, all minimal words for $\varphi(wx_v)$ are equivalent to each other, and the statement holds.

Now assume that $g(v-1) < g(v)$. In this case, $I(g\sigma_v) = I(g) + 1$, and wx_v is a minimal word for $\varphi(wx_v)$. Thus, we have to show that every other minimal word w' for $\varphi(wx_v)$ is equivalent to wx_v . Let us consider sequentially three alternative possibilities for the rightmost letter of w' : either it is x_v , or it is $x_{v\pm 1}$, or it is x_μ , where $|\mu - v| \geq 2$. In the first case, $w' = ux_v$, where u is a minimal word for g . Since w is a minimal word for g as well and $\ell(w) = \ell(u) \leq m$, the induction hypothesis implies that $u \sim w$. Therefore, $w' = ux_k \sim wx_k$ as well.

Now consider the second case, assuming that $w' = ux_{v+1}$ (for $w' = ux_{v-1}$ the argument is completely symmetric). Since both words wx_v , ux_{v+1} are minimal for $g\sigma_v$, the permutation $g\sigma_v$ sends a triple of sequential elements $v-1$, v , $v+1$ to

$$g(v) > g(v-1) > g(v+1),$$

whereas the permutation g sends them to

$$g(v-1) < g(v) > g(v+1).$$

Therefore, $g\sigma_v$ has a minimal word of the form $sx_{v+1}x_vx_{v+1}$, and g has a minimal word of the form tx_vx_{v+1} (because of $g(v-1) > g(v+1)$). The permutation $h = \varphi(s) = \varphi(t)$ sends elements $v-1$, v , $v+1$ to

$$g(v+1) < g(v-1) < g(v)$$

and has $I(h) = I(g\sigma_v) - 3 = I(g) - 2$. Thus both words t , s are minimal for h and are equivalent by the induction hypothesis. At the same time, $w \sim tx_vx_{v+1}$. Hence, $wx_v \sim tx_vx_{v+1}x_v \sim sx_vx_{v+1}x_v \sim sx_{v+1}x_vx_{v+1}$. On the other hand, $sx_{v+1}x_v \sim u$, because both words are minimal for the same permutation, which sends $v-1$, v , $v+1$ to

$$g(v) > g(v+1) < g(v-1)$$

(where $g(v) > g(v-1)$) and has inversion index $I(g\sigma_v) - 1$. We conclude that $wx_v \sim ux_{v+1}$, as required.

Finally, let $g\sigma_v = \varphi(wx_v) = \varphi(ux_\mu)$, where $|\mu - v| \geq 2$. Then two disjoint pairs of sequential elements $v-1$, v and $\mu-1$, μ are sent by $g\sigma_v$ to $g(v-1) > g(v)$ and $g(\mu-1) > g(\mu)$. Therefore, $g\sigma_v$ has minimal words looking like $tx_\mu x_v$ and $sx_v x_\mu$, where both t , s are minimal for the permutation $h = \varphi(t) = \varphi(s)$, which sends pairs $v-1$, v and $\mu-1$, μ to $g(v) < g(v-1)$ and $g(\mu) < g(\mu-1)$ respectively. By the induction hypothesis, $t \sim s$, because $I(h) = I(g\sigma_v) - 2 = m - 1$, and $w \sim tx_\mu$, because both words are minimal for g . A similar argument shows that $sx_v \sim u$. (Both words sx_v , u are minimal for the permutation $\varphi(sx_v) = \varphi(u)$, which differs from h

by a transposition in the first of two pairs and has inversion number $I(g\sigma_v) - 1 = m$.) We conclude that $wx_v \sim tx_\mu x_v \sim sx_\mu x_v \sim sx_v x_\mu \sim ux_\mu$, as required. \square

13.3 Simple Groups and Composition Series

A group G is called *simple* if G has no normal subgroups different from $\{e\}$ and G . For example, every finite group of prime order is simple, because its only subgroups are the trivial group of one element and the entire group by Lagrange's theorem, Theorem 12.3. Since normal subgroups are exactly the kernels of homomorphisms, a group G is simple if and only if every group homomorphism $G \rightarrow G'$ is either injective or trivial, i.e., takes the whole group G to the unit of G' .

13.3.1 Jordan–Hölder Series

A finite strictly decreasing sequence of subgroups

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_{n-1} \supsetneq G_n = \{e\}$$

is called a *Jordan–Hölder* (or *composition*) *series* of the group G if for each i , the subgroup G_{i+1} is normal within G_i and the quotient group G_i/G_{i+1} is simple. In this case, the quotient groups G_i/G_{i+1} , $0 \leq i \leq n-1$, are called *Jordan–Hölder* (or *composition*) *factors* of G . The cardinality n of the total collection of all Jordan–Hölder factors (where repeated elements are allowed as well) is called the *composition length*¹⁷ of the group G . A group allowing a finite composition series is called a *finite-length group*.

Example 13.1 (Composition Factors of S_4) We have seen above that S_4 admits the following composition series:

$$S_4 \supset A_4 \supset V_4 \supset \mathbb{Z}/(2) \supset \{e\},$$

where $A_4 \triangleleft S_4$ is the subgroup of even permutations, $V_4 \triangleleft A_4$ is the Klein four group,¹⁸ and $\mathbb{Z}/(2) \triangleleft V_4 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ is any of three cyclic subgroups of order 2 spanned by nonunit elements. Therefore, S_4 has four Jordan–Hölder factors: $\mathbb{Z}/(2) = S_4/A_4$, $\mathbb{Z}/(3) = A_4/V_4$, $\mathbb{Z}/(2) = V_4/(\mathbb{Z}/(2))$, and $\mathbb{Z}/(2) = \mathbb{Z}/(2)/\{e\}$. Thus, the composition length of S_4 is 4. Note that three of the four Jordan–Hölder factors of S_4 coincide.

¹⁷Or just *length* for short.

¹⁸Consisting of the identity and three pairs of disjoint transpositions of cyclic type $\begin{smallmatrix} \square & \square \\ \square & \square \end{smallmatrix}$.

Exercise 13.14 Check that $A_4/V_4 \simeq \mathbb{Z}/(3)$.

Theorem 13.1 (Jordan–Hölder Theorem) *If a group G admits a finite composition series, then the nonordered total collection of all Jordan–Hölder factors does not depend on the choice of composition series. In particular, the composition length is well defined for every group of finite length.*

Proof Let the group G have two Jordan–Hölder series

$$G = P_0 \supsetneq P_1 \supsetneq P_2 \supsetneq \cdots \supsetneq P_{n-1} \supsetneq P_n = \{e\}, \quad (13.9)$$

$$G = Q_0 \supsetneq Q_1 \supsetneq Q_2 \supsetneq \cdots \supsetneq Q_{m-1} \supsetneq Q_m = \{e\}. \quad (13.10)$$

Our plan is to insert some chains of *nonstrictly* decreasing subgroups between sequential elements of both series in such a way that the resulting two collections of sequential quotients will be in a natural bijection such that all the corresponding quotients are isomorphic. Since each quotient is either zero or some Jordan–Hölder factor of G , this leads to a one-to-one correspondence between the composition factors coming from (13.9) and (13.10).

It follows from Proposition 12.5 on p. 302 applied to the normal subgroup $P_{i+1} \triangleleft P_i$ and just a subgroup $Q_v \cap P_i \subset P_i$ that for each i , there exists a chain of subgroups

$$P_i \supseteq (Q_1 \cap P_i)P_{i+1} \supseteq (Q_2 \cap P_i)P_{i+1} \supseteq \cdots \supseteq (Q_{m-1} \cap P_i)P_{i+1} \supseteq P_{i+1}, \quad (13.11)$$

which starts from P_i , ends with P_{i+1} , and has $(Q_{k+1} \cap P_i)P_{i+1} \triangleleft (Q_k \cap P_i)P_{i+1}$ with

$$\frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}. \quad (13.12)$$

Exercise 13.15 (Zassenhaus’s Butterfly Lemma) Let some group have four subgroups A, B, C, D such that $A \triangleleft B$ and $C \triangleleft D$. Deduce from Proposition 12.5 on p. 302 that there exists an isomorphism $(B \cap D)C / (A \cap D)C \simeq (B \cap D) / (A \cap D)(B \cap C)$ and use it to prove (13.12).

The subgroup P_{i+1} is normal within all subgroups of the chain (13.11). Taking quotients, we get

$$\frac{P_i}{P_{i+1}} \supseteq \frac{(Q_1 \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \frac{(Q_2 \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \cdots \supseteq \frac{(Q_{m-1} \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \{e\}, \quad (13.13)$$

where each subgroup is normal within the preceding one, and the sequential factors

$$\frac{(Q_k \cap P_i)P_{i+1}/P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}/P_{i+1}} \simeq \frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}$$

coincide with (13.12). Since the quotient group P_i/P_{i+1} is simple, all inclusions in the chain (13.13) are equalities except for exactly one strict inequality; that is, all sequential quotients in (13.12) are trivial except for exactly one, isomorphic to P_i/P_{i+1} .

The same argument applied to Q instead of P allows us to insert a nonstrictly decreasing chain of subgroups

$$Q_k \supseteq (P_1 \cap Q_k)Q_{k+1} \supseteq (P_2 \cap Q_k)Q_{k+1} \supseteq \cdots \supseteq (P_{n-1} \cap Q_k)Q_{k+1} \supseteq Q_{k+1} \quad (13.14)$$

between any two sequential elements $Q_k \supset Q_{k+1}$ in the composition series (13.10). In (13.14), each group is a normal subgroup within the preceding, and the sequential quotients

$$\frac{(P_i \cap Q_k)Q_{k+1}}{(P_{i+1} \cap Q_k)Q_{k+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})} \quad (13.15)$$

are isomorphic to the corresponding quotients in (13.12). Thus, after insertion of chains (13.11), (13.14) between neighboring members of the series (13.9), (13.10), we get two chains of equal length equipped with a natural bijection between sequential quotients such that the corresponding factors (13.15) and (13.12) are isomorphic. Since Q_{k+1} is a normal subgroup of all groups in (13.14), we can factor the chain (13.14) through it and apply the same arguments as used for P_{i+1} and the chain (13.11). They show that for every fixed k , there is precisely one nonunit quotient among the factors (13.15), and it is isomorphic to Q_k/Q_{k+1} . \square

Remark 13.1 A group of finite length may have many different composition series in which the Jordan–Hölder factors of the group may appear in different orders. Furthermore, two finite-length groups with equal collections of Jordan–Hölder factors are not necessarily isomorphic.

13.3.2 Finite Simple Groups

One of the foremost mathematical achievements of the twentieth century was completing the list of all finite simple groups. It consists of several infinite series and 26 so-called *sporadic* simple groups lying outside the series.¹⁹ The infinite series are of three types: cyclic additive groups $\mathbb{Z}/(p)$ of simple order, even permutation groups A_n for²⁰ $n \geq 5$, and the simple linear algebraic groups over finite fields.²¹ The

¹⁹The Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$, but not M_{10} are among them (see [Problem 12.34](#) on p. 306).

²⁰However, $A_3 \simeq \mathbb{Z}/(3)$ is also simple.

²¹Such as $\mathrm{PSL}_n(\mathbb{F}_q)$. Explicit definitions and classifying theorems for these groups can be found in textbooks on linear algebraic and/or arithmetic groups, e.g. *Linear Algebraic Groups*, by James E. Humphreys [[Hu](#)].

enumeration of all finite simple groups was accomplished by collecting the results of hundreds of papers written by scores of researchers who had been working in diverse directions.²² The last gaps were filled in only in 2008. A more or less universal viewpoint that could treat the classification of finite simple groups uniformly has yet to be developed. Below, we will prove the simplicity of the even permutation groups A_n for $n \geq 5$.

Lemma 13.1 *The group A_5 is simple.*

Proof Two permutations are conjugate in S_5 if and only if they have equal cyclic types. The cyclic types of even permutations are

$$\begin{array}{c} \square\square\square\square\square, \quad \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & & \\ \hline \end{array}, \quad \begin{array}{|c|c|} \hline \square & \square \\ \hline \square & \square \\ \hline \end{array}, \quad \begin{array}{|c|} \hline \square \\ \hline \square \\ \hline \square \\ \hline \square \\ \hline \end{array}. \end{array} \quad (13.16)$$

i.e., 5-cycles, 3-cycles, pairs of disjoint transpositions, and the identity. The corresponding conjugacy classes in S_5 have cardinalities $5!/5 = 24$, $5!/(3 \cdot 2) = 20$, $5!/(2^2 \cdot 2) = 15$, and 1.

Exercise 13.16 Verify that every permutation of the last three types commutes with an odd permutation.

Therefore, the permutations of the last three types are conjugate in S_5 if and only if they are conjugate in A_5 . Hence, the last three classes are conjugacy classes within A_5 as well. Cycles of length 5 split into two conjugacy classes within A_5 : 12 cycles conjugate to $[1, 2, 3, 4, 5]$ and 12 cycles conjugate to $[2, 1, 3, 4, 5]$.

Exercise 13.17 Check this.

Every normal subgroup $H \triangleleft A_5$ either contains the entire nonunit conjugacy class or is disjoint from it. Therefore, $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$, where each coefficient ε_k equals either 1 or 0. At the same time, $|H|$ divides $|A_5| = 60 = 3 \cdot 4 \cdot 5$.

Exercise 13.18 Verify that this is possible only in two cases: either for all $\varepsilon_k = 1$ or for all $\varepsilon_k = 0$.

Thus, the normal subgroups in A_5 are exhausted by the trivial subgroup consisting of the identity and the whole of A_5 . \square

Theorem 13.2 *The groups A_n are simple for all $n \geq 5$.*

Proof By induction on n . Let $N \triangleleft A_n$. The stabilizer $\text{Stab}_{A_n}(k)$ of an element k is clearly isomorphic to A_{n-1} . By the induction hypothesis, the subgroup

$$N \cap \text{Stab}_{A_n}(k) \triangleleft \text{Stab}_{A_n}(k)$$

²²The final part of the story is expounded in a six-volume manuscript [GLS].

is either $\{e\}$ or the whole of $\text{Stab}_{A_n}(k)$. Since the stabilizers of all elements are conjugate, the subgroup N either contains all stabilizers or intersects each stabilizer trivially. In the first case, N contains all pairs of disjoint transpositions, and therefore $N = A_n$.

Exercise 13.19 Verify that A_n is generated by the pairs of disjoint transpositions.

In the second case, for every $i \neq j$, there is at most one $g \in N$ such that $g(i) = j$.

Exercise 13.20 For $n \geq 6$, let $g \in A_n$ take $g(i) = j \neq i$. Show that there exists $h \neq g$ that is conjugate to g in A_n and takes $h(i) = j$ as well.

Since N is normal, it cannot have any nonidentity permutations, i.e., $N = \{e\}$. \square

13.4 Semidirect Products

13.4.1 Semidirect Product of Subgroups

Recall that we put $NH \stackrel{\text{def}}{=} \{xh \mid x \in N, h \in H\}$ for subsets $N, H \subset G$. When N and H are subgroups of G , the multiplication map $N \times H \rightarrow NH$, $(x, h) \mapsto xh$, becomes bijective if and only if $N \cap H = \{e\}$. Indeed, if $N \cap H = \{e\}$ and $x_1h_1 = x_2h_2$, then $x_2^{-1}x_1 = h_2h_1^{-1} \in N \cap H$ is forced to be e , and therefore $x_2 = x_1$, $h_2 = h_1$. Conversely, if $N \cap H$ contains some $z \neq e$, then distinct pairs (e, e) and (z, z^{-1}) are both mapped to e .

Two subgroups $N, H \subset G$ are called *complementary* if $N \cap H = \{e\}$ and $NH = G$. In this case, every element $g \in G$ can be uniquely factored as $g = xh$. If, in addition, the subgroup $N \triangleleft G$ is normal, then we say that G is the *semidirect product* of N and H , and we write²³ $G = N \rtimes H$. In this case,

$$(x_1h_1)(x_2h_2) = x_1(h_1x_2h_1^{-1}) \cdot h_1h_2 \quad \text{in } G,$$

where $x_1(h_1x_2h_1^{-1}) \in N$, $h_1h_2 \in H$. Thus, we can treat the composition in G as a composition on the set $N \times H$, which differs from the componentwise composition within N and H and is defined as

$$(x_1, h_1) \cdot (x_2, h_2) \stackrel{\text{def}}{=} (x_1 \text{Ad}_{h_1}(x_2), h_1h_2), \quad (13.17)$$

where $\text{Ad}_h : N \rightarrow N$, $x \mapsto h x h^{-1}$, means the adjoint action²⁴ of an element h on N . If the adjoint action of H on N is trivial, i.e., $xh = hx$ for every $x \in N$, $h \in H$, then the semidirect product becomes the *direct* product with the usual componentwise composition $(x_1, h_1) \cdot (x_2, h_2) = (x_1x_2, h_1h_2)$.

²³The symbol \rtimes should serve as a reminder that $N \triangleleft N \rtimes H$.

²⁴See Example 12.14 on p. 295.

Example 13.2 ($D_n \simeq \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$) The dihedral group D_n contains the normal subgroup of rotations, which is isomorphic to the additive group $\mathbb{Z}/(n)$. The cyclic group of order 2 spanned by a reflection is complementary to the subgroup of rotations and is isomorphic to the additive group $\mathbb{Z}/(2)$. The adjoint action of a reflection on a rotation changes the direction of the rotation. After identification of rotations and reflections with residue classes, this action becomes an action of $\mathbb{Z}/(2)$ on $\mathbb{Z}/(n)$ such that the classes $[0]_2, [1]_2 \in \mathbb{Z}/(2)$ act as multiplication by $+1$ and -1 respectively. Thus, $D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$, and in terms of residue class pairs $(x, y) \in \mathbb{Z}/(n) \times \mathbb{Z}/(2)$, composition in D_n is described by the formula $(x_1, y_1) \cdot (x_2, y_2) = (x_1 + (-1)^{y_1} x_2, y_1 + y_2)$, where $x_1, x_2 \in \mathbb{Z}/(n)$, $y_1, y_2 \in \mathbb{Z}/(2)$.

Example 13.3 ($\text{Aff}(V) \simeq V \rtimes \text{GL}(V)$) We have seen in Example 12.21 on p. 301 that the group $\text{Aff}(V)$ of affine automorphisms of the affinization $\mathbb{A}(V)$ of a vector space V contains a normal subgroup of shifts $\tau_v : x \mapsto x + v$, which is isomorphic to the additive group of V . On the other hand, the stabilizer $\text{Stab}_{\text{Aff}(V)}(p)$ of a point $p \in \mathbb{A}(V)$ is identified with the general linear group $\text{GL}(V)$ by means of the vectorization map $\text{vec}_p : \mathbb{A}(V) \rightarrow V$, $q \mapsto \overrightarrow{pq}$, with the origin at p . Since the stabilizer $\text{Stab}_{\text{Aff}(V)}(p)$ does not contain nonzero shifts and every affine map $F : \mathbb{A}(V) \rightarrow \mathbb{A}(V)$ can be decomposed as $F = \tau_v \circ G$ for $v = \overrightarrow{pF(p)} \in V$ and $G = \tau_{-v} \circ F \in \text{Stab}_{\text{Aff}(V)}(p)$, we conclude that the affine group $\text{Aff}(V)$ is the semidirect product of the subgroup of shifts $V \triangleleft \text{Aff}(V)$ and the general linear group $\text{GL}(V)$ embedded in $\text{Aff}(V)$ as the stabilizer of some point $p \in \mathbb{A}(V)$. By Exercise 12.27 on p. 301, the adjoint action of $\text{GL}(V)$ on shifts coincides with the tautological action of linear maps on vectors. Therefore, in terms of the pairs $(v, F) \in V \times \text{GL}(V)$, the composition in $\text{Aff}(V) \simeq V \rtimes \text{GL}(V)$ is given by the formula $(u, F) \cdot (w, G) = (u + F(w), FG)$.

13.4.2 Semidirect Product of Groups

A composition of type (13.17) can be defined for any two abstract groups N, H , not necessarily given as complementary subgroups of some ambient group. In this general setup, instead of the adjoint action, we consider an arbitrary action of a group H on a group G by group automorphisms, i.e., any group homomorphism

$$\psi : H \rightarrow \text{Aut } N, \quad h \mapsto \psi_h : N \rightarrow N. \quad (13.18)$$

Given such an action, we equip the direct product of sets $N \times H$ with the binary operation

$$(x_1, h_1) \cdot (x_2, h_2) \stackrel{\text{def}}{=} (x_1 \psi_{h_1}(x_2), h_1 h_2). \quad (13.19)$$

Exercise 13.21 Check that the composition (13.19) provides $N \times H$ with a group structure with unit (e, e) and inverses given by $(x, h)^{-1} = (\psi_h^{-1}(x^{-1}), h^{-1})$, where $\psi_h^{-1} = \psi_{h^{-1}} : N \xrightarrow{\sim} N$ is the group automorphism inverse to $\psi_h : N \xrightarrow{\sim} N$.

The resulting group is called the *semidirect product* of the groups N, H with respect to the action $\psi : N \rightarrow \text{Aut } H$ and is denoted by $N \rtimes_\psi H$. Let me stress that the semidirect product actually depends on the choice of ψ . For example, if ψ is trivial, that is, $\psi_h = \text{Id}_N$ for all h , then $N \rtimes_\psi H = N \times H$ is the usual direct product with componentwise composition.

Exercise 13.22 Check that for every semidirect product $G = N \rtimes_\psi H$:
(a) $N' = \{(x, e) \mid x \in N\}$ is a normal subgroup of G isomorphic to N , and $G/N' \simeq H$,
(b) $H' = \{(e, h) \mid h \in H\}$ is the subgroup of G complementary to N' , and $G = N' \rtimes H'$.

13.5 p -Groups and Sylow's Theorems

13.5.1 p -Groups in Action

Every finite group of order p^n , where $p \in \mathbb{N}$ is prime, is called a p -group. Every subgroup of a p -group is itself a p -group by Lagrange's theorem.²⁵ In particular, the stabilizer of a point in an arbitrary action of a p -group is a p -group, and therefore, the length of every orbit is either divisible by p or equal to 1. This leads to a simple but very useful claim:

Proposition 13.5 Every action of a p -group G on a finite set X such that $p \nmid |X|$ has a fixed point.

Proof Since the length of every orbit cannot be divisible by p , there is some orbit of length 1. □

Proposition 13.6 Every p -group G has a nontrivial center

$$Z(G) = \{c \in G \mid \forall g \in G \, cg = gc\}.$$

Proof The center $Z(G)$ is the fixed-point set of the adjoint action²⁶ of G on itself. Since the lengths of all orbits in $G \setminus Z(G)$ are divisible by p , it follows that $|Z(G)| = |G| - |G \setminus Z(G)|$ is divisible by p and positive, because $e \in Z(G)$. □

Exercise 13.23 Show that every group of order p^2 is abelian.

²⁵See Theorem 12.3 on p. 300.

²⁶See Example 12.14 on p. 295.

13.5.2 Sylow Subgroups

Let G be an arbitrary finite group. Write its order as $|G| = p^n m$, where $p, n, m \in \mathbb{N}$, p is prime, and $\gcd(m, p) = 1$. A subgroup $S \subset G$ of order $|S| = p^n$ is called a *Sylow p -subgroup*. The total number of the Sylow p -subgroups in G is denoted by $N_p(G)$.

Theorem 13.3 (Sylow's Theorem) *For every finite group G and prime divisor p of $|G|$ there exists a Sylow p -subgroup in G . Every p -subgroup of G is contained in some Sylow p -subgroup. All Sylow p -subgroups are conjugate.*

Proof Let $|G| = p^n m$, where $\gcd(m, p) = 1$ as above. Write \mathcal{E} for the set of all subsets of cardinality p^n in G . The group G acts on \mathcal{E} by left multiplication: an element $g \in G$ maps $X \mapsto gX = \{gx \mid x \in X\}$. For every $F \in \mathcal{E}$, $F \subset G$, the stabilizer $\text{Stab}(F) = \{g \in G \mid gF = F\}$ acts on the set F by left multiplication. This action is free, because $g_1 x \neq g_2 x$ for $g_1 \neq g_2$ in the group G . Since each orbit consists of $|\text{Stab}(F)|$ points, $p^n = |F|$ is divisible by $|\text{Stab}(F)|$. We come to the following two alternatives for the length of a G -orbit of a point $F \in \mathcal{E}$ under the action of G on \mathcal{E} : it is either divisible by p or equal to m .

If the second case occurs for some F , then $|\text{Stab}(F)| = p^n$, i.e., $\text{Stab}(F) \subset G$ is a Sylow p -subgroup. By Proposition 13.5, the action of any p -subgroup $H \subset G$ on the length- m orbit of F has some fixed point gF . This means that $H \subset \text{Stab}(gF) = g \text{Stab}(F) g^{-1}$, i.e., H is contained in some Sylow p -subgroup conjugate to $\text{Stab}(F)$. If H itself is Sylow, i.e., $|H| = p^n$, then this inclusion is an equality.

If the first case occurs for all $F \in \mathcal{E}$, then the lengths of all orbits in the action $G : \mathcal{E}$ are divisible by p . This is impossible, because $|\mathcal{E}| = \binom{p^n m}{p^n} \equiv m \pmod{p}$ is coprime to p by Exercise 2.10 on p. 29. \square

Corollary 13.1 (Addendum to Sylow's Theorem) $N_p \mid m$ and $N_p \equiv 1 \pmod{p}$ for every prime divisor p of $|G|$.

Proof Write \mathcal{S} for the set of all Sylow p -subgroups in G and consider the adjoint action of G on \mathcal{S} , in which $g \in G$ maps $H \mapsto gHg^{-1}$. This action is transitive by Sylow's theorem. Therefore, $|\mathcal{S}| = |G|/|\text{Stab}(P)|$ for every $P \in \mathcal{S}$. Since $P \subset \text{Stab}(P)$, we conclude that $|P| = p^n$ divides $|\text{Stab}(P)|$. This forces $|\mathcal{S}|$ to divide $|G|/p^n = m$ and proves the first statement. To prove the second it is enough to check that the adjoint action of a p -group P on \mathcal{S} has exactly one fixed point, namely P itself. In this case, the lengths of all the other orbits are multiples of p , and we obtain the required congruence $|\mathcal{S}| \equiv 1 \pmod{p}$. Let $H \in \mathcal{S}$ be fixed by P . Then $P \subset \text{Stab}(H) = \{g \in G \mid gHg^{-1} \subset H\}$. By Lagrange's theorem, the inclusions $H \subset \text{Stab}(H) \subset G$ force $|\text{Stab}(H)| = p^n m'$, where $m' \mid m$ and $\gcd(m', p) = 1$. Therefore, both P and H are Sylow p -subgroups of $\text{Stab}(H)$. Since all Sylow p -subgroups are conjugate and H is normal in $\text{Stab}(H)$, we conclude that $H = P$. \square

Example 13.4 (Groups of Order pq for $\text{GCD}(p-1, q) = 1$) Let $|G| = pq$, where $p > q$ and both p, q are prime. Then G has exactly one Sylow p -subgroup $H_p \simeq \mathbb{Z}/(p)$, and it is normal. Every Sylow q -subgroup $H_q \simeq \mathbb{Z}/(q)$ has $H_p \cap H_q = e$, because both groups H_p and H_q are simple. Hence, the multiplication map

$$H_p \times H_q \rightarrow H_p H_q \subset G$$

is injective, and therefore $H_p H_q = G$ by a cardinality argument. We conclude that H_q is complementary to H_p . By Sect. 13.4, this forces

$$G = H_p \rtimes H_q \simeq \mathbb{Z}/(p) \rtimes_{\psi} \mathbb{Z}/(q)$$

for some action $\psi : \mathbb{Z}/(q) \rightarrow \text{Aut}(\mathbb{Z}/(p))$.

Exercise 13.24 Verify that for every coprime $m, n \in \mathbb{Z}$, there are no nontrivial homomorphisms of additive groups $\mathbb{Z}/(m) \rightarrow \mathbb{Z}/(n)$.

By Exercise 12.4 on p. 280, $\text{Aut}(\mathbb{Z}/(p)) \simeq \mathbb{F}_p^*$. For $\text{GCD}(p-1, q) = 1$, the above exercise implies that every action of $\mathbb{Z}/(q)$ on $\mathbb{Z}/(p)$ is trivial. Hence,

$$G \simeq \mathbb{Z}/(p) \oplus \mathbb{Z}/(q)$$

if q is coprime to $p-1$.

Example 13.5 (Groups of Order $2p$) Let $|G| = 2p$ for prime $p > 2$. The same arguments as in the previous example show that $G = \mathbb{Z}/(p) \rtimes_{\psi} \mathbb{Z}/(2)$ for some action $\psi : \mathbb{Z}/(2) \rightarrow \text{Aut}(\mathbb{Z}/(p)) \simeq \mathbb{F}_p^*$. The latter is completely determined by an element $\psi([1]) \in \mathbb{F}_p^*$ such that $\psi([1])^2 = 1$. There are exactly two such elements: $\psi([1]) = 1$ and $\psi([1]) = -1$. For the first choice, the action ψ is trivial, and $G \simeq \mathbb{Z}/(p) \oplus \mathbb{Z}/(2)$. In the second case, the classes $[0]_2, [1]_2 \in \mathbb{Z}/(2)$ act on $\mathbb{Z}/(p)$ as multiplication by $+1$ and -1 respectively. Thus, $G \simeq D_p$ by Example 13.2 on p. 329.

Problems for Independent Solution to Chap. 13

Problem 13.1 Show that for $n \geq 3$, the group A_n is generated by the 3-cycles

$$(k-2, k-1, k), 3 \leq k \leq n.$$

Problem 13.2 Enumerate all conjugacy classes in A_6 and indicate their cardinalities.

Problem 13.3 Which conjugacy classes of the even permutations in S_n split into several distinct conjugacy classes within A_n ?

Problem 13.4 Show that the center of S_n is trivial for $n \geq 3$.

Problem 13.5 (Simplicity of SO_3) Let $G = SO_3(\mathbb{R})$ be the rotation group²⁷ of the Euclidean space \mathbb{R}^3 . For every $v \in \mathbb{R}^3$ and $\varphi \in \mathbb{R}$, write $R_{v,\varphi} \in G$ for rotation about the axis spanned by v by the angle φ in the clockwise direction as it looks in the direction of v . Check that $FR_{v,\varphi}F^{-1} = R_{Fv,\varphi}$ for all $F \in G$ and use this to prove that the group G is simple.

Problem 13.6 Show that the complete group O_{C^n} of the standard n -cocube²⁸ $C^n \subset \mathbb{R}^n$:

- (a) is presented by generators x_1, x_2, \dots, x_n and relators $x_i^2 = (x_i x_j)^2$, $(x_{k-1} x_k)^3$, $(x_{n-1} x_n)^4$ for all $1 \leq i, j \leq n$ such that $|i - j| \geq 2$ and all $2 \leq k \leq n - 1$, where the generators act on C^n by reflections $\sigma_1, \sigma_2, \dots, \sigma_n$ in hyperplanes $\pi_n = e_n^\perp$ and $\pi_i = (e_i - e_{i+1})^\perp$, $1 \leq i \leq (n - 1)$.
- (b) is isomorphic to the semidirect product $(\mathbb{Z}/2)^n \rtimes S_n$, where S_n acts on $(\mathbb{Z}/2)^n$ by permutations of coordinates.

Problem 13.7 Describe the automorphism groups of the following groups:

- (a) $\mathbb{Z}/(n)$, (b) $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$, (c) D_3 , (d) D_4 , (e) Q_8 .

Problem 13.8 Which groups in the previous problem have no outer automorphisms?

Problem 13.9 Let two actions $\varphi, \psi : H \rightarrow \text{Aut } N$ be related as $\varphi = \text{Ad}_g \circ \psi$ for some $g \in N$. Show that $N \rtimes_\psi H \simeq N \rtimes_\varphi H$.

Problem 13.10 Let p be the smallest prime divisor of $|G|$. Show that every subgroup of index p in G is normal.²⁹

Problem 13.11 Show that every group of even order contains an element of order 2.

Problem 13.12 For a group of order p^n , show that every subgroup of order p^k , $k < n$, is contained in some subgroup of order p^{k+1} .

Problem 13.13 Is there a simple group of order 12?

Problem 13.14 Describe all groups of order ≤ 15 up to isomorphism.

²⁷See Example 10.13 on p. 247.

²⁸See Problem 10.13 on p. 250.

²⁹For example, every subgroup of index 2 is normal, every subgroup of index 3 in a group of odd order is normal, etc.

Problem 13.15 Show that there are exactly three mutually nonisomorphic nondirect semidirect products $\mathbb{Z}/(8) \rtimes \mathbb{Z}/(2)$.

Problem 13.16 Describe all groups of order 55.

Problem 13.17 Use the action of G on its Sylow 5-subgroups to show that A_5 is the only simple group of order 60.

Problem 13.18 Give an example of two nonisomorphic groups $G_1 \not\cong G_2$ and normal subgroups $H_1 \triangleleft G_1, H_2 \triangleleft G_2$ such that $G_1/H_1 \cong G_2/H_2$.

Chapter 14

Modules over a Principal Ideal Domain

In this chapter, K by default means an arbitrary commutative ring with unit and \mathbb{k} means an arbitrary field. A K -module always means a unital module over K .

14.1 Modules over Commutative Rings Revisited

Recall¹ that a *unital module* over a commutative ring K with unit is an additive abelian group M equipped with multiplication by constants

$$K \times M \rightarrow M$$

possessing all the properties of multiplication of vectors by scalars in a vector space that were listed in Definition 6.1 on p. 123. An abelian subgroup $N \subset M$ is called a K -submodule if $\lambda a \in N$ for all $\lambda \in K$ and all $a \in N$. Submodules $N \subsetneq M$ are called *proper*. If $N \subset M$ is a submodule, then the quotient module M/N consists of congruence classes

$$[m]_N = m \pmod{N} = m + N = \{m' \in M \mid m' - m \in N\},$$

which can be viewed as equivalence classes modulo the relation $m \sim m'$, meaning that $m' - m \in N$. These classes are added and multiplied by constants by the standard rules

$$[m_1] + [m_2] \stackrel{\text{def}}{=} [m_1 + m_2] \quad \text{and} \quad \lambda[m] \stackrel{\text{def}}{=} [\lambda m].$$

¹See Definition 6.2 on p. 124.

Exercise 14.1 Check that both operations are well defined and satisfy all axioms from Definition 6.1 on p. 123.

A *homomorphism* of K -modules² is a homomorphism of abelian groups $\varphi : M \rightarrow N$ that respects multiplication by scalars, i.e., such that $\varphi(\lambda v) = \lambda\varphi(v)$ for all $\lambda \in K$ and all $v, w \in M$. Homomorphisms of modules possess all the properties valid for homomorphisms of abelian groups. In particular,³ $\varphi(0) = 0$, $\varphi(v - w) = \varphi(v) - \varphi(w)$ for all $v, w \in M$; all nonzero fibers $\varphi^{-1}(\varphi(v)) = v + \ker \varphi$ are congruence classes modulo the kernel $\ker \varphi = \{a \in M \mid \varphi(a) = 0\}$; the image $\operatorname{im} \varphi = \varphi(M)$ is isomorphic to $M / \ker \varphi$; etc. In particular, φ is injective if and only if $\ker \varphi = 0$.

All K -linear maps $M \rightarrow N$ form a K -module, denoted by $\operatorname{Hom}(M, N)$. If a precise reference to the ground ring K is needed, we write $\operatorname{Hom}_K(M, N)$. The addition of homomorphisms and their multiplication by constants are defined by the same rules as for linear maps of vector spaces: given $f, g : M \rightarrow N$ and $\lambda, \mu \in K$, then $\lambda f + \mu g : m \mapsto \lambda f(m) + \mu g(m)$.

14.1.1 Free Modules

Recall that a subset $E \subset M$ is called a *basis* of M if each vector $w \in M$ has a unique linear expression $w = \sum e \in E x_e e$, where $x_e \in K$ and all but a finite number of the x_e are equal to zero.

Exercise 14.2 Check that a set of vectors is a basis if and only if it is linearly independent and spans the module.

If a module has a basis, it is called a *free module*. For example, all coordinate modules K^n are free for every ring K . All vector spaces over a field \mathbb{k} are free \mathbb{k} -modules by Theorem 6.1 on p. 132. In Sect. 6.2 on p. 127, we saw some other examples of free modules. Elements of a free module with basis E can be thought of as functions $x : E \rightarrow K$ with finite support.

Lemma 14.1 *A subset $E \subset M$ is a basis of a K -module M if and only if for every K -module N and every map of sets $\varphi : E \rightarrow N$, there exists a unique homomorphism of K -modules $f_\varphi : M \rightarrow N$ that extends φ .*

Proof If E is a basis, then every K -linear map $f_\varphi : M \rightarrow N$ that maps $e \mapsto \varphi(e)$ should take $f(\sum e \in E x_e e) = \sum e \in E x_e \varphi(e)$. On the other hand, the prescription $(x_e)_{e \in E} \mapsto \sum e \in E x_e \varphi(e)$ actually defines a K -linear map from a free module with basis E to N .

Exercise 14.3 Check this.

²Also called a K -linear map.

³See Sect. 2.6 on p. 31.

Now assume that $E \subset M$ satisfies the second condition and write N for the free K -module with basis E . Then the identity map $\text{Id}_E : E \rightarrow E$ is uniquely extended to K -linear maps $f : M \rightarrow N$ and $g : N \rightarrow M$. Since composition $gf : M \rightarrow M$ acts identically on $E \subset M$, it coincides with the identity map Id_M by our assumption. Since N is free, the composition $fg : N \rightarrow N$ coincides with Id_N for the same reason. Thus, f and g are mutually inverse isomorphisms, i.e., $M \simeq N$ is free. \square

Exercise 14.4 Show that $\text{Hom}(K^m, N) \simeq N^{\oplus m}$ (direct sum of m copies of N).

14.1.2 Generators and Relations

If the ground ring K is not a field, then not all K -modules are free. A common way to represent a nonfree K -module M is to choose linear generators for M and list all the linear relations between them. Then the vectors of M can be treated as linear combinations of the chosen generators considered up to the listed linear relations. This is formalized as follows.

Associated with a collection of vectors $\mathbf{w} = (w_1, w_2, \dots, w_m) \in M$ is a linear map

$$\pi_{\mathbf{w}} : K^m \rightarrow M, \quad e_i \mapsto w_i, \quad (14.1)$$

which sends $(x_1, x_2, \dots, x_m) \in K^m$ to the linear combination

$$x_1 w_1 + x_2 w_2 + \dots + x_m w_m \in M.$$

The vectors w_1, w_2, \dots, w_m are linearly independent if and only if $\pi_{\mathbf{w}}$ is injective. They span M if and only if $\pi_{\mathbf{w}}$ is surjective. In the latter case, $M \simeq K^m / R_{\mathbf{w}}$, where $R_{\mathbf{w}} \stackrel{\text{def}}{=} \ker \pi_{\mathbf{w}}$ is a submodule formed by the coefficients (x_1, x_2, \dots, x_m) of all linear relations $x_1 w_1 + x_2 w_2 + \dots + x_m w_m = 0$ in M . For this reason, $R_{\mathbf{w}}$ is called a *module of relations* between generators w_1, w_2, \dots, w_m . Note that by construction, $R_{\mathbf{w}}$ is a submodule of a free module. Thus, an arbitrary finitely generated K -module over a ring K can be written as K^m / R for appropriate $m \in \mathbb{N}$ and $R \subset K^m$.

Example 14.1 (Ideals) Every commutative ring K is clearly a K -module. A subset $I \subset K$ is a submodule if and only if I is an ideal of K . A principal ideal $(a) \subset K$ is a free K -module if and only if the generator a is not a zero divisor. Every nonprincipal ideal is generated by at least two elements, which are linearly related, because any two elements $a, b \in K$ are linearly related, e.g., as $a \cdot b - b \cdot a = 0$. For example, the ideal $I = (x, y) \subset \mathbb{Q}[x, y]$ considered as a module over the polynomial ring $K = \mathbb{Q}[x, y]$ cannot be generated by one element, because x, y have no nonconstant common divisors. The epimorphism $\pi_{(x,y)} : K^2 \twoheadrightarrow I, (f, g) \mapsto xf + yg$, associated with the generators x, y has free kernel $R_{(x,y)} = \ker \pi_{(x,y)}$ with basis $(y, -x)$, because the equality $xf = -yg$ forces $f = yh, g = -xh$ for some $h \in \mathbb{Q}[x, y]$, since $\mathbb{Q}[x, y]$ is factorial, and therefore every K -linear relation between x and y is proportional to $(y, -x)$. We conclude that $I \simeq K^2 / K \cdot (y, -x)$ as a K -module.

Example 14.2 (Abelian Groups) Every abelian group A has a canonical \mathbb{Z} -module structure defined by

$$(\pm n) \cdot a \stackrel{\text{def}}{=} \pm \underbrace{(a + a + \cdots + a)}_{n \text{ summands}}$$

for $n \in \mathbb{N}$, $a \in A$, and $0 \cdot a = 0$ for all $a \in A$.

Exercise 14.5 Verify the axioms from Definition 6.1 on p. 123.

For the additive group of residue classes $M = \mathbb{Z}/(k)$, such multiplication by integers yields $n \cdot [m]_k = [nm]_k$, where $[x]_k = x \pmod{k}$ denotes the residue class of $x \in \mathbb{Z}$ modulo k . Therefore, M is generated over \mathbb{Z} by one element $[1]_k$ satisfying the nontrivial linear relation $k \cdot [1]_k = 0$. Thus, $[1]_k$ is not a *basis* for M , just a linear generator. The epimorphism (14.1) provided by this generator is nothing but the quotient map $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(k)$, $n \mapsto [n]_k$, with kernel $R = (k)$, and the representation $M \simeq K^m/R = \mathbb{Z}/(k)$ is a tautology. The linear relation $k \cdot [1]_k = 0$ prohibits nonzero homomorphisms $\varphi : \mathbb{Z}/(k) \rightarrow \mathbb{Z}$. Indeed, $k \cdot \varphi([1]_k) = \varphi(k \cdot [1]_k) = \varphi(0) = 0$ forces $\varphi([1]_k) = 0$, because \mathbb{Z} has no zero divisors. Then $\varphi([m]_k) = \varphi(m \cdot [1]_k) = m \cdot \varphi([1]_k) = 0$ for every residue class $[m]_k$.

Exercise 14.6 Show that $[n]_k$ linearly generates $\mathbb{Z}/(k)$ over \mathbb{Z} if and only if

$$\text{GCD}(n, k) = 1.$$

14.1.3 Linear Maps

Let a K -module M be spanned by vectors w_1, w_2, \dots, w_m . Then every K -linear map $F : M \rightarrow N$ is uniquely determined by its values $u_i = F(w_i)$ on these generators, because every vector $v = x_1 w_1 + x_2 w_2 + \cdots + x_m w_m \in M$ should be sent to

$$F(v) = F(x_1 w_1 + x_2 w_2 + \cdots + x_m w_m) = x_1 u_1 + x_2 u_2 + \cdots + x_m u_m. \quad (14.2)$$

However, not every set of vectors $u_1, u_2, \dots, u_m \in N$ allows us to construct a K -linear homomorphism $F : M \rightarrow N$ such that $F(w_i) = u_i$. For example, we have seen in Example 14.2 that there are no nonzero \mathbb{Z} -linear maps $\mathbb{Z}/(k) \rightarrow \mathbb{Z}$ at all.

Proposition 14.1 *If the vectors w_1, w_2, \dots, w_m span the module M , then for every collection of vectors u_1, u_2, \dots, u_m in a K -module N , there exists at most one homomorphism $F : M \rightarrow N$ such that $F(w_i) = u_i$. It exists if and only if for every linear relation $\lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_m w_m = 0$ in M , the same relation $\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_m u_m = 0$ holds in N . In this case, F is well defined by the formula (14.2).*

Proof The collection of vectors $u_1, u_2, \dots, u_m \in N$ is the same as the map

$$\{e_1, e_2, \dots, e_m\} \rightarrow N$$

from the standard basis of K^m to N . By Lemma 14.1, such maps are in bijection with the K -linear maps $K^m \rightarrow N$. Under this bijection, the collection $\mathbf{u} = (u_1, u_2, \dots, u_m)$ corresponds to the map

$$F_{\mathbf{u}} : (x_1, x_2, \dots, x_m) \mapsto x_1 u_1 + x_2 u_2 + \dots + x_m u_m.$$

It is factored through the quotient module $M = K^m / R_{\mathbf{w}}$ as

$$\begin{array}{ccc} K^m & \xrightarrow{F_{\mathbf{u}}} & N \\ & \searrow & \nearrow F \\ & M & \end{array}$$

if and only if $R_{\mathbf{w}} \subset \ker F_{\mathbf{u}}$, which means precisely that for all $(x_1, x_2, \dots, x_m) \in K^m$,

$$x_1 w_1 + x_2 w_2 + \dots + x_m w_m = 0 \quad \Rightarrow \quad x_1 u_1 + x_2 u_2 + \dots + x_m u_m = 0.$$

If this holds, then F has to be defined by the formula (14.2). \square

14.1.4 Matrices of Linear Maps

Let K -modules M and N be spanned by the vectors

$$\mathbf{w} = (w_1, w_2, \dots, w_m) \quad \text{and} \quad \mathbf{u} = (u_1, u_2, \dots, u_n)$$

respectively. For every K -linear map $F : M \rightarrow N$, write $F_{\mathbf{u}\mathbf{w}} \in \text{Mat}_{n \times m}(K)$ for the matrix whose j th column is formed by the coefficients of some linear expansion of the vector Fw_j through the generators u_i . Therefore, $(Fw_1, Fw_2, \dots, Fw_m) = (u_1, u_2, \dots, u_n) \cdot F_{\mathbf{u}\mathbf{w}}$. If the generators u_i are linearly related, then such a matrix is not unique. Thus, the notation $F_{\mathbf{u}\mathbf{w}}$ is not quite correct. If the generators w_j are linearly related, then not every matrix in $\text{Mat}_{n \times m}(K)$ is the matrix of the linear map $F : M \rightarrow N$. Nevertheless, if we are given a well-defined homomorphism of K -modules $F : M \rightarrow N$, then for every choice of the matrix $F_{\mathbf{u}\mathbf{w}}$ and linear expansion $v = \sum w_j x_j = \mathbf{w} \cdot \mathbf{x}$, where $\mathbf{x} = (x_1, x_2, \dots, x_m)^t$, the image $F(v)$ certainly can be linearly expanded through generators \mathbf{u} as $F(v) = \mathbf{u} \cdot F_{\mathbf{u}\mathbf{w}} \mathbf{x}$.

Proposition 14.2 *Let a K -module M be generated by the vectors (w_1, w_2, \dots, w_m) and suppose the linear endomorphism $F : V \rightarrow V$ sends them to*

$$(Fw_1, Fw_2, \dots, Fw_m) = (w_1, w_2, \dots, w_m) \cdot F_w,$$

where $F_w \in \text{Mat}_m(K)$. Then the image of the homothety

$$\det F_w : V \rightarrow V, v \mapsto v \cdot \det F_w,$$

is contained in $\text{im } F$.

Proof Multiplication by $\det F_w$ acts on the generating vectors by the rule

$$(w_1, w_2, \dots, w_m) \mapsto (w_1, w_2, \dots, w_m) \cdot \det F_w \cdot E = (w_1, w_2, \dots, w_m) \cdot F_w \cdot F_w^\vee,$$

where E is the identity matrix and F_w^\vee is the adjunct matrix⁴ of F_w . Since the columns of $F_w \cdot F_w^\vee$ are in the linear span of the columns of F_w , multiplication by $\det F_w$ sends each w_i into $\text{im } F$. \square

Example 14.3 (Another Proof of the Cayley–Hamilton Identity) Recall that for $A \in \text{Mat}_n(K)$ and $f(t) = f_0 + f_1 t + \dots + f_m t^m \in K[x]$, we write

$$f(A) \stackrel{\text{def}}{=} f_0 E + f_1 A + f_2 A^2 + \dots + f_m A^m \in \text{Mat}_n(K)$$

for the result of the *evaluation*⁵ of f at A in $\text{Mat}_n(K)$. For an arbitrary matrix $A \in \text{Mat}_n(K)$, consider the coordinate K -module K^n , whose elements will be written in columns, and equip it with a $K[t]$ -module structure by the rule

$$f(t) \cdot v \stackrel{\text{def}}{=} f(A) v = f_0 v + f_1 A v + f_2 A^2 v + \dots + f_m A^m v. \quad (14.3)$$

Exercise 14.7 Verify the axioms from Definition 6.1 on p. 123.

The standard basis vectors e_1, e_2, \dots, e_n of K^n span K^n over $K[t]$ as well. However, over $K[t]$, they are linearly related. In particular, the homothety with coefficient t : $v \mapsto tv$ has two different matrices in this system of generators: one equals $t \cdot E$, while the other equals A . As a result, the zero map, which takes each vector to zero, can be represented by the nonzero matrix $tE - A$. It follows from Proposition 14.2 that multiplication by $\det(tE - A) = \chi_A(t)$ annihilates K^n . In accordance with the definition (14.3), multiplication by the polynomial $\chi_A(t)$ considered as a K -linear map $K^n \rightarrow K^n$ has matrix $\chi_A(A)$ in the standard basis of K^n . Since K^n is free over K , each K -linear endomorphism of K^n has a unique matrix in the standard basis. We conclude that $\chi_A(A) = 0$.

⁴See Sect. 9.6 on p. 220.

⁵See Sect. 8.1.3 on p. 175.

14.1.5 Torsion

Everywhere in this section, we assume that K has no zero divisors. An element m of a K -module M is called a *torsion element* if $\lambda m = 0$ for some nonzero $\lambda \in K$.

Exercise 14.8 Verify that the torsion elements form a submodule of M .

The submodule of all torsion elements in M is denoted by

$$\text{Tors } M \stackrel{\text{def}}{=} \{m \in M \mid \exists \lambda \neq 0 : \lambda m = 0\}$$

and called the *torsion submodule*. A module M is called *torsion-free* if $\text{Tors } M = 0$. For example, every ideal in K is torsion-free under our assumption that K has no zero divisors. Of course, every free K -module is torsion-free.

Exercise 14.9 Show that if N is torsion-free, then every K -linear map $f : M \rightarrow N$ annihilates $\text{Tors}(M)$.

If $\text{Tors } M = M$, then M is called a *torsion module*. For example, the quotient ring K/I by a nonzero ideal $I \subset K$ is a torsion K -module, because $\lambda[x]_I = [\lambda x]_I = 0$ for every nonzero $\lambda \in I$.

14.1.6 Quotient of a Module by an Ideal

For an ideal $I \subset K$ and K -module M , we write $IM \subset M$ for the submodule formed by all finite linear combinations of vectors in M with coefficients in I :

$$IM \stackrel{\text{def}}{=} \{x_1 a_1 + x_2 a_2 + \cdots + x_n a_n \mid x_i \in I, a_i \in M, n \in \mathbb{N}\}.$$

Exercise 14.10 Verify that IM is actually a K -submodule in M .

The quotient module M/IM has the structure of a module over the quotient ring K/I defined by

$$[\lambda]_I \cdot [w]_{IM} \stackrel{\text{def}}{=} [\lambda w]_{IM},$$

where $[\lambda]_I = \lambda \pmod{I}$ and $[a]_{IM} = a \pmod{IM}$.

Exercise 14.11 Verify the consistency of this multiplication rule.

14.1.7 Direct Sum Decompositions

A direct sum (respectively product) of modules is defined as the direct sum (respectively product) of the underlying abelian groups equipped with componentwise

multiplication by scalars exactly as was done for vector spaces in Sect. 6.4.5 on p. 141.

Exercise 14.12 Show that the direct sum of free modules with bases E and F is a free module with basis $E \sqcup F$.

Associated with any collection of submodules $N_1, N_2, \dots, N_s \subset M$ is the K -linear *addition map*

$$N_1 \oplus N_2 \oplus \cdots \oplus N_s \rightarrow M, \quad (u_1, u_2, \dots, u_s) \mapsto u_1 + u_2 + \cdots + u_s. \quad (14.4)$$

If it is bijective, then M is said to be the *direct sum* of the submodules N_i . We write $M = \oplus_i N_i$ in this case. Bijectivity of the addition map (14.4) means that every vector $w \in M$ has a unique decomposition $w = u_1 + u_2 + \cdots + u_s$ with $u_i \in N_i$. For example, a free K -module with basis e_1, e_2, \dots, e_n is the direct sum of n free modules $K \cdot e_i$ with bases e_i :

$$K^n = Ke_1 \oplus Ke_2 \oplus \cdots \oplus Ke_n.$$

Exercise 14.13 Let $M = L \oplus N$ for submodules $L, N \subset M$. Show that $M/N \simeq L$.

Lemma 14.2 Given two submodules $L, N \subset M$, then $M = L \oplus N$ if and only if $L \cup N$ spans M and $L \cap N = 0$.

Proof $L \cup N$ spans M if and only if the addition map

$$\sigma : L \oplus N \rightarrow M, \quad (a, b) \mapsto a + b,$$

is surjective. The kernel of the addition map is zero if and only if $L \cap N = 0$, because $(a, b) \in \ker \sigma$ if and only if $a = -b \in L \cap N$. \square

Exercise 14.14 Show that for every direct sum decomposition $M = M_1 \oplus M_2 \oplus \cdots \oplus M_m$ and ideal $I \subset K$, we have $IM = IM_1 \oplus IM_2 \oplus \cdots \oplus IM_m$ and

$$M/IM = (M_1/IM_1) \oplus (M_2/IM_2) \oplus \cdots \oplus (M_m/IM_m).$$

Theorem 14.1 Let M be a free module over a commutative ring K with unit. Then all bases in M have the same cardinality.

Proof Choose a maximal ideal⁶ $\mathfrak{m} \subset K$ and consider the quotient module $M/\mathfrak{m}M$ as a vector space over the field $\mathbb{k} = K/\mathfrak{m}$. If a set $E \subset M$ is a basis of M over K , then

$$M = \bigoplus_{e \in E} K \cdot e, \quad \mathfrak{m}M = \bigoplus_{e \in E} \mathfrak{m} \cdot e, \quad \text{and} \quad M/\mathfrak{m}M = \bigoplus_{e \in E} \mathbb{k} \cdot e.$$

⁶See Sect. 5.2.2 on p. 107.

Hence, E is a basis of the vector space $M/\mathfrak{m}M$ over \mathbb{k} . Since the vector space $M/\mathfrak{m}M$ does not depend on E , and by Theorem 6.1 on p. 132, all bases of $M/\mathfrak{m}M$ over \mathbb{k} have the same cardinality, we conclude that the cardinality of the basis in M does not depend on the choice of this basis. \square

Definition 14.1 (Rank of a Free Module) The cardinality of a basis of a free module M is called the *rank* of M and is denoted by $\text{rk } M$.

Remark 14.1 It follows from the proof of Theorem 14.1 that $\dim_{\mathbb{k}} M/\mathfrak{m}M = \text{rk } M$. Since the right-hand side does not depend on $\mathfrak{m} \subset K$ and is well defined by Theorem 14.1, $\dim_{\mathbb{k}} (M/\mathfrak{m}M)$ is the same for all maximal ideals $\mathfrak{m} \subset K$.

Definition 14.2 (Decomposability) A module M is called *decomposable* if there exist proper submodules $L, N \subset M$ such that $M = L \oplus N$. Otherwise, M is called *indecomposable*.

Example 14.4 Let us show that \mathbb{Z} is an indecomposable \mathbb{Z} -module. The proper submodules $L \subset \mathbb{Z}$ are exhausted by the principal ideals $L = (d)$. If there is a submodule $N \subset \mathbb{Z}$ such that $\mathbb{Z} = (d) \oplus N$, then $N \simeq \mathbb{Z}/(d)$ by Exercise 14.13. Since \mathbb{Z} is torsion-free, there is no inclusion $N \subset \mathbb{Z}$. Contradiction.

Exercise 14.15 For $M = \mathbb{Z}^2$ and the \mathbb{Z} -submodule $N \subset M$ generated by the vectors $(2, 1)$ and $(1, 2)$, show that $N \simeq \mathbb{Z}^2$, $M/N \simeq \mathbb{Z}/(3)$, and that there exists no \mathbb{Z} -submodule $L \subset M$ such that $M = L \oplus N$.

14.1.8 Semisimplicity

A module M is called *semisimple* if for every nonzero proper submodule $N \subset M$, there exists a submodule $L \subset M$ such that $M = L \oplus N$. Every submodule L with this property is said to be *complementary* to N .

Exercise 14.16 Show that every vector space V over an arbitrary field \mathbb{k} is semisimple.

If a commutative ring K is not a field, then there exist nonsemisimple modules. We have seen above that the free \mathbb{Z} -modules \mathbb{Z} and \mathbb{Z}^2 are not semisimple. An example of a semisimple \mathbb{Z} -module is $M = \mathbb{Z}/(p) \oplus \mathbb{Z}/(p) \oplus \cdots \oplus \mathbb{Z}/(p)$, where $p \in \mathbb{N}$ is prime. This module is simultaneously a vector space over the field $\mathbb{F}_p = \mathbb{Z}/(p)$, and all its \mathbb{Z} -submodules are at the same time vector subspaces over \mathbb{F}_p and conversely. In particular, every vector subspace complementary to N serves as a complementary \mathbb{Z} -submodule as well.

14.2 Invariant Factors

14.2.1 Submodules of Finitely Generated Free Modules

Beginning from this point, we assume by default that the ground ring K is a principal ideal domain⁷ and all free K -modules in question are finitely generated. A free module of rank zero always means for us the zero module.

Lemma 14.3 *Let M be a free module of rank $m < \infty$ over an arbitrary principal ideal domain K . Then every submodule $N \subset M$ is free, and $\text{rk } N \leq \text{rk } M$.*

Proof By induction on $m = \text{rk } M$. If $m = 1$, then $M \simeq K$, and the submodule $N \subset M$ is the principal ideal $(d) \subset K$. If $d = 0$, then $N = 0$ is free of rank 0. If $d \neq 0$, then $(d) = d \cdot K$ is free of rank 1 with basis⁸ d . Now consider $m > 1$. Let us fix some basis e_1, e_2, \dots, e_m in M and write vectors $w \in M$ as the rows of coordinates in this basis. Then the first coordinates $x_1(v)$ of all vectors $v \in N$ form an ideal $(d) \subset K$. If $d = 0$, then N is contained in the free module $M' \subset M$ with basis e_2, \dots, e_m . By induction, N is free with $\text{rk } N \leq (m - 1)$. If $d \neq 0$, write $v_1 \in N$ for some vector whose first coordinate equals d . Then $N = K \cdot v_1 \oplus N'$, where $N' = N \cap M'$ consists of the vectors with vanishing first coordinate, because $(K \cdot v_1) \cap N' = 0$ and every vector $v \in N$ can be decomposed as $\lambda v_1 + w$ for $\lambda = x_1(v)/d$ and $w = v - \lambda v_1 \in N'$. By induction, N' is free of rank at most $m - 1$. The module Kv_1 is free of rank 1 with basis v_1 , because $\lambda v_1 \neq 0$ for $\lambda \neq 0$. Hence, N is free of rank at most m . \square

Theorem 14.2 (Invariant Factors Theorem) *Let K be a principal ideal domain, M a free K -module of rank $m < \infty$, and $N \subset M$ a submodule, automatically free of rank $n \leq m$ by Lemma 14.3. Then there exists a basis e_1, e_2, \dots, e_m in M such that appropriate multiples $f_1 e_1, f_2 e_2, \dots, f_n e_n$ of the first n basis vectors form a basis in N and satisfy the divisibility conditions $f_i \mid f_j$ for all $i < j$. The factors f_i considered up to multiplication by invertible elements do not depend on the choice of such a basis.*

Definition 14.3 (Reciprocal Bases and Invariant Factors) Bases e_1, e_2, \dots, e_m in M and $f_1 e_1, f_2 e_2, \dots, f_n e_n$ in N satisfying the conditions of Theorem 14.2 are called *reciprocal bases* of M and $N \subset M$. The factors $f_1, f_2, \dots, f_n \in K$ considered up to multiplication by invertible elements are called the *invariant factors* of the submodule $N \subset M$.

We split the proof of Theorem 14.2 into a few steps presented in Sects. 14.2.2–14.2.4 below. To begin, we give an equivalent reformulation of Theorem 14.2 in terms of matrices.

⁷See Sect. 5.3 on p. 109.

⁸Note that d is linearly independent, because K has no zero divisors: $\lambda d = 0 \Rightarrow \lambda = 0$.

Theorem 14.3 (Smith Normal Form Theorem) *For every rectangular matrix $C \in \text{Mat}_{m \times k}(K)$, there exists a pair of invertible matrices $F \in \text{GL}_m(K)$, $G \in \text{GL}_k(K)$ such that the matrix*

$$D = FCG = \begin{pmatrix} f_1 & & & 0 \\ & \ddots & & \\ 0 & & f_n & \\ & & & 0 \end{pmatrix} \quad (14.5)$$

has $d_{ij} = 0$ for all $i \neq j$, and all nonzero diagonal elements $f_i \stackrel{\text{def}}{=} d_{ii}$ satisfy the divisibility conditions $f_i \mid f_j$ for all $i < j$. The nonzero diagonal elements f_i of the matrix D considered up to multiplication by invertible elements of K do not depend on the choice of matrices F, G satisfying (14.5) and the divisibility conditions on f_i .

Definition 14.4 (Smith Normal Form) The diagonal matrix D from Theorem 14.3 is called the *Smith normal form* of the matrix C . The nonzero diagonal elements f_1, f_2, \dots, f_n in Smith normal form are called *invariant factors* of the matrix C .

14.2.2 Deduction of the Invariant Factors Theorem from the Smith Normal Form Theorem

Let us fix a basis $\mathbf{w} = (w_1, w_2, \dots, w_m)$ of M and vectors $\mathbf{u} = (u_1, u_2, \dots, u_k)$ spanning N . We apply Theorem 14.3 to the transition matrix $C_{\mathbf{w}\mathbf{u}} \in \text{Mat}_{k \times m}$, whose j th column is the column coordinates of the vector u_j in the basis \mathbf{w} . Thus, $\mathbf{u} = \mathbf{w} \cdot C_{\mathbf{w}\mathbf{u}}$. Let $F \in \text{GL}_m(K)$, $G \in \text{GL}_k(K)$ fit the conditions of Theorem 14.3 for $C = C_{\mathbf{w}\mathbf{u}}$, that is, the matrix $D = FC_{\mathbf{w}\mathbf{u}}G$ has diagonal form (14.5) and satisfies the required divisibility conditions. Since F is invertible, the vectors $\mathbf{e} = \mathbf{w}F^{-1}$ also form a basis of M . The vectors $\varepsilon \stackrel{\text{def}}{=} \mathbf{u}G$ are expressed through \mathbf{e} as $\varepsilon = \mathbf{u}G = \mathbf{w}C_{\mathbf{w}\mathbf{u}}G = \mathbf{e}FC_{\mathbf{w}\mathbf{u}}G = \mathbf{e}D$. Hence, only the first n vectors in ε are nonzero. These nonzero vectors $\varepsilon_i = f_i e_i$ are linearly independent, because the vectors e_i are. They span N , because the initial generators \mathbf{u} are linearly expressed through ε as $\mathbf{u} = \varepsilon G^{-1}$. Therefore, $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ is a basis of N . This proves the existence of reciprocal bases. If there are two bases $\mathbf{e}' = (e'_1, e'_2, \dots, e'_m)$ and $\mathbf{e}'' = (e''_1, e''_2, \dots, e''_m)$ in M such that some multiples $\varepsilon'_i = f'_i e'_i$ and $\varepsilon''_i = f''_i e''_i$ for $1 \leq i \leq n$ form bases in N and satisfy the required divisibility conditions, then both diagonal transition matrices $C_{\varepsilon''\mathbf{e}''} = C_{\varepsilon''\mathbf{e}'} C_{\varepsilon'\mathbf{e}'} C_{\mathbf{e}'\mathbf{e}''}$ and $C_{\varepsilon'\mathbf{e}'} = E_n C_{\varepsilon'\mathbf{e}''} E_m$, where E_n, E_m are the identity $n \times n$ and $m \times m$ matrices, fit the conditions of Theorem 14.3 for the same $n \times m$ matrix $C = C_{\varepsilon'\mathbf{e}'}$. Hence, $f'_i = f''_i$ up to multiplication by invertible elements.

14.2.3 Uniqueness of the Smith Normal Form

Write $\Delta_k(C) \in K$ for the greatest common divisor⁹ of all $k \times k$ minors in a matrix C . For a diagonal matrix (14.5) such that $f_i \mid f_j$ for all $j < i$, we have $\Delta_k(D) = f_1 f_2 \dots f_k$. Thus, the diagonal elements $f_k = \Delta_k(D)/\Delta_{k-1}(D)$ are recovered from the quantities $\Delta_k(D)$ uniquely up to multiplication by invertible elements. The uniqueness of the Smith normal form of a matrix C follows now from the next lemma.

Lemma 14.4 *The numbers $\Delta_k(C) \in K$ (considered up to multiplication by invertible elements of K) are not changed under multiplication of C by an invertible matrix from either side.*

Proof Since $\Delta_k(C) = \Delta_k(C')$, it is enough to consider left multiplication. Let $F = AC$, where A is invertible. Since the rows of F are K -linear combinations of the rows of C , every order- k minor in F is a K -linear combination of order- k minors in C .

Exercise 14.17 Check this explicitly.

This forces $\Delta_k(C)$ to divide $\Delta_k(F)$. For the same reason, the equality $C = A^{-1}F$ forces $\Delta_k(F)$ to divide $\Delta_k(C)$. Therefore, $\Delta_k(C)$ and $\Delta_k(F)$ coincide up to an invertible factor.¹⁰ \square

14.2.4 Gaussian Elimination over a Principal Ideal Domain

We will construct matrices F, G satisfying Theorem 14.3 as products

$$F = F_r F_{r-1} \dots F_1, \quad G = G_1 \cdot G_2 \dots G_s$$

of some elementary invertible matrices F_v (respectively G_v) such that the transformation $A \mapsto F_v A$ (respectively $A \mapsto A G_v$) changes just two rows (respectively columns) a_i, a_j in A and leaves all the other rows (respectively columns) of A fixed. Rows (respectively columns) a_i, a_j will be replaced by their linear combinations $a'_i = \alpha a_i + \beta a_j, a'_j = \gamma a_i + \delta a_j$. Such a replacement is invertible if and only if $\alpha\delta - \beta\gamma = 1$. In that case, the elementary matrix F_v (respectively G_v) is invertible too. We call such invertible transformations of pairs of rows (respectively columns) *generalized Gaussian operations*.¹¹

⁹Recall that the greatest common divisor of elements in a principal ideal domain is a generator of the ideal spanned by those elements. It is unique up to multiplication by invertible elements of K (see Sect. 5.3.2 on p. 110).

¹⁰Compare with Exercise 5.17 on p. 111.

¹¹Compare with Sect. 8.4 on p. 182.

Lemma 14.5 *For every pair of elements (p, q) in the same row (respectively column) of a matrix A and such that $p \nmid q$ and $q \nmid p$, there exists a generalized Gaussian column operation (respectively row operation) that transforms (p, q) to $(d, 0)$, where $d = \text{GCD}(p, q)$.*

Proof Write $d = \text{GCD}(p, q)$ as $d = px + qy$. Then $p = ad$, $q = bd$ for some $a, b \in K$, and we have the equalities $bp = aq$ and $ax + by = 1$, which imply that

$$(p, q) \cdot \begin{pmatrix} x & -b \\ y & a \end{pmatrix} = (d, 0), \quad \begin{pmatrix} x & y \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix},$$

and

$$\det \begin{pmatrix} x & -b \\ y & a \end{pmatrix} = \det \begin{pmatrix} x & y \\ -b & a \end{pmatrix} = ax + by = 1.$$

□

To finish the proof of Theorem 14.3, it remains to establish the next proposition.

Proposition 14.3 *Every $m \times n$ matrix C over an arbitrary principal ideal domain K can be transformed to Smith normal form (14.5) by means of generalized Gaussian operations on rows and columns.*

Proof After an appropriate permutation of rows and columns, we may assume that $c_{11} \neq 0$. If all elements of C are divisible by c_{11} , then the usual elementary row and column operations allow us to eliminate the first column and the first row of C outside the upper left cell. Induction on the size of C allows us to transform the remaining $(m-1) \times (n-1)$ submatrix to Smith form. During this transformation, all matrix elements remain divisible by c_{11} .

Now assume that C contains an element $a \notin (c_{11})$. Let $d = \text{GCD}(a, c_{11})$. We are going to transform C into a matrix C' such that $c'_{11} = d$. Note that this transformation strictly enlarges the ideal generated by the upper left cell, because $(c_{11}) \subsetneq (a, c_{11}) = (c'_{11})$. If a is in the first row or in the first column, it is enough to change the pair (c_{11}, a) by $(d, 0)$ via Lemma 14.5. If all elements in the first row and the first column of C are divisible by c_{11} and a is strictly to the right and below c_{11} , then at the first step, we eliminate the first column and the first row of C outside the upper left cell by means of the usual elementary row and column operations. This changes a by its sum with some multiple of c_{11} , so the resulting element remains indivisible by c_{11} . We continue to write a for this element. At the second step, we add the row containing a to the first row and get a pair (c_{11}, a) in the first row. Finally, we change this pair by $(d, 0)$ via Lemma 14.5.

Since K is Noetherian,¹² the ideal generated by the upper left cell of C cannot be strictly enlarged infinitely many times. Therefore, after a few transformations as

¹²See Definition 5.1 on p. 104.

described above, we come to some matrix C all of whose elements are divisible by c_{11} . This case was already considered at the beginning of the proof. \square

Exercise 14.18 Form a Γ -shaped table $\begin{array}{|c|c|} \hline C & E \\ \hline E & \\ \hline \end{array}$ by attaching the $m \times m$ and $n \times n$ identity matrices on the right and at the bottom of C . Then transform C to Smith normal form by applying the generalized row and column operations to the whole Γ -shaped table. Write $\begin{array}{|c|c|} \hline D & F \\ \hline G & \\ \hline \end{array}$ for the resulting table. Show that the matrices $D = FCG$ satisfy Theorem 14.3.

Example 14.5 (Abelian Subgroups in \mathbb{Z}^m) By Lemma 14.3, every abelian subgroup $L \subset \mathbb{Z}^m$ is a free \mathbb{Z} -module. Let $\text{rk } L = \ell$. By Theorem 14.2, there exists a basis u_1, u_2, \dots, u_m in \mathbb{Z}^m such that some multiples $m_1 u_1, m_2 u_2, \dots, m_\ell u_\ell$ of the first ℓ basis vectors form a basis in L . This means, in particular, that for the quotient \mathbb{Z}^m/L , we have

$$\mathbb{Z}^m/L \simeq \frac{\mathbb{Z}}{(m_1)} \oplus \cdots \oplus \frac{\mathbb{Z}}{(m_\ell)} \oplus \mathbb{Z}^{m-\ell}. \quad (14.6)$$

Let us carry out this analysis in detail for the subgroup $L \subset \mathbb{Z}^3$ spanned by the columns of the matrix

$$C = \begin{pmatrix} 126 & 51 & 72 & 33 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix}. \quad (14.7)$$

To find reciprocal bases, we have to transform this matrix to Smith normal form. The GCD of all matrix elements equals 3. We can get -3 at the $(1, 4)$ cell by subtracting the second row multiplied by 4 from the first row. With Exercise 14.18 in mind, we

perform this operation in the Γ -shaped table $\begin{array}{|c|c|} \hline C & E \\ \hline E & \\ \hline \end{array}$ and get

$$\begin{pmatrix} 6 & -9 & 0 & -3 & 1 & -4 & 0 \\ 30 & 15 & 18 & 9 & 0 & 1 & 0 \\ 60 & 30 & 36 & 18 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \end{pmatrix}.$$

Then we change the sign in the first row and swap the first and the fourth columns:

$$\begin{pmatrix} 3 & 9 & 0 & -6 & -1 & 4 & 0 \\ 9 & 15 & 18 & 30 & 0 & 1 & 0 \\ 18 & 30 & 36 & 60 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 1 & 0 & 0 & 0 & & & \end{pmatrix}.$$

Now we can eliminate the first column and the first row of C outside the upper left-hand cell by subtracting appropriate multiples of the first row from the other rows and then doing the same with the columns:

$$\begin{pmatrix} 3 & 0 & 0 & 0 & -1 & 4 & 0 \\ 0 & -12 & 18 & 48 & 3 & -11 & 0 \\ 0 & -24 & 36 & 96 & 6 & -24 & 1 \\ 0 & 0 & 0 & 1 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 1 & -3 & 0 & 2 & & & \end{pmatrix}.$$

Now eliminate the third row of C by subtracting the doubled second row and add the third column to the second in order to extract the GCD of the second row:

$$\begin{pmatrix} 3 & 0 & 0 & 0 & -1 & 4 & 0 \\ 0 & 6 & 18 & 48 & 3 & -11 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 1 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 1 & 1 & 0 & & & \\ 1 & -3 & 0 & 2 & & & \end{pmatrix}.$$

It remains to eliminate the third and the fourth columns in C by adding appropriate multiples of the second column:

$$\begin{pmatrix} 3 & 0 & 0 & 0 & -1 & 4 & 0 \\ 0 & 6 & 0 & 0 & 3 & -11 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 1 & & & \\ 0 & 1 & -3 & -8 & & & \\ 0 & 1 & -2 & -8 & & & \\ 1 & -3 & 9 & 26 & & & \end{pmatrix}.$$

Thus, the Smith normal form D of the matrix C from (14.7) is

$$D = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 4 & 0 \\ 3 & -11 & 0 \\ 0 & -2 & 1 \end{pmatrix} \cdot C \cdot \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & -8 \\ 0 & 1 & -2 & -8 \\ 1 & -3 & 9 & 26 \end{pmatrix}.$$

This means that $L \simeq \mathbb{Z}^2$ and $\mathbb{Z}^3/L \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}$. A basis of L is formed by the vectors

$$3v_1 = c_4 \quad \text{and} \quad 6v_2 = c_2 + c_3 - 3c_4, \quad (14.8)$$

where c_j means the j th column of the matrix C and v_j means the j th column of the matrix

$$F^{-1} = \begin{pmatrix} -1 & 4 & 0 \\ 3 & -11 & 0 \\ 0 & -2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 11 & 4 & 0 \\ 3 & 1 & 0 \\ 6 & 2 & 1 \end{pmatrix},$$

whose columns form a basis of \mathbb{Z}^3 reciprocal to the sublattice L . The right-hand sides of formulas (14.8) are the first two columns of the matrix CG , i.e., the reciprocal basis vectors of L .

Exercise 14.19 Show that the following properties of a sublattice $L \subset \mathbb{Z}^m \subset \mathbb{Q}^m$ spanned by the columns of a matrix $C \in \text{Mat}_{m \times n}(\mathbb{Z})$ are equivalent: **(a)** $\text{rk } L = m$, **(b)** \mathbb{Z}^m/L is finite, **(c)** L spans \mathbb{Q}^m over \mathbb{Q} , **(d)** C as a matrix over \mathbb{Q} has rank m .

Example 14.6 (Commensurable Lattices) An abelian subgroup $L \subset \mathbb{Z}^m$ satisfying the equivalent conditions from Exercise 14.19 is called *commensurable* with \mathbb{Z}^m . If L is given as the \mathbb{Z} -linear span of columns of some integer rectangular matrix C , then L is commensurable with \mathbb{Z}^m if and only if $\text{rk } C = m$. Note that this can be checked by the standard Gaussian elimination over \mathbb{Q} as in Sect. 8.4 on p. 182.

Proposition 14.4 Let an abelian subgroup $L \subset \mathbb{Z}^n$ be spanned by the columns of a square matrix $C \in \text{Mat}_n(\mathbb{Z})$. Then L is commensurable with \mathbb{Z}^n if and only if $\det C \neq 0$. In this case, $|\mathbb{Z}^n/L| = |\det C|$, i.e., the cardinality of the quotient \mathbb{Z}^n/L is equal to the Euclidean volume of the parallelepiped spanned by any basis of L .

Proof Choose a basis u_1, u_2, \dots, u_n in \mathbb{Z}^n such that some multiples

$$m_1 u_1, m_2 u_2, \dots, m_\ell u_\ell$$

form a basis in L . We have seen in Sect. 14.2.2 that the $n \times n$ diagonal matrix D with $d_{ii} = m_i$ for $1 \leq i \leq \ell$ satisfies the matrix equality $FCG = D$, where $F, G \in$

$\text{Mat}_n(\mathbb{Z})$ are invertible. This means that $|\det F| = |\det G| = 1$. Thus $|\det C| = |\det D|$ vanishes if and only if $\ell < n$. If $\ell = n$, then $|\det C| = m_1 \cdot m_2 \cdots m_n$ equals the cardinality of the quotient $\mathbb{Z}^n/L = \bigoplus_i \mathbb{Z}/(m_i)$. \square

14.3 Elementary Divisors

14.3.1 Elementary Divisors Versus Invariant Factors

Associated with every sequence of elements $f_1, f_2, \dots, f_n \in K$ such that $f_i \mid f_j$ for all $i < j$ is the disjoint union of all positive integer powers of irreducible elements $p_{ij}^{m_{ij}}$ appearing in the prime factorizations $f_i = p_{i1}^{m_{i1}} p_{i2}^{m_{i2}} \cdots p_{ik_i}^{m_{ik_i}}$, where $1 \leq i \leq n$, all p_{ij} are considered up to multiplication by invertible elements of K , and $(p_{ij}) \neq (p_{ik})$ for each i and $j \neq k$. The unordered disjoint union of all these $p_{ij}^{m_{ij}}$ is called the *collection of elementary divisors*¹³ of the sequence of invariant factors f_1, f_2, \dots, f_n . For example, the sequence of integer invariant factors 6, 6, 12, 108 produces the following collection of elementary divisors: 2, 2, 2², 2², 3, 3, 3, 3³.

Lemma 14.6 *The correspondence described above establishes a bijection between the finite sequences $f_1, f_2, \dots, f_n \in K$, where each f_i is considered up to multiplication by invertible elements of K and $f_i \mid f_j$ for all $i < j$, and the finite unordered collections of (possibly repeated) positive integer powers p^μ of irreducible elements $p \in K$, where two collections are considered equal if they are in one-to-one correspondence such that the corresponding powers p^μ and q^ν have $\mu = \nu$ and $p = sq$ for some invertible $s \in K$.*

Proof We have to show that every sequence of invariant factors f_1, f_2, \dots, f_n is uniquely recovered from the collection of its elementary divisors. For every prime $p \in K$, write $m(p)$ and $n(p)$, respectively, for the maximal exponent of p and for the total number of (possibly repeated) powers of p represented in the collection of divisors. Now let us place the divisors in the cells of an appropriate Young diagram as follows. Choose a prime p_1 with maximal $n(p_1)$ and write in a row all its powers represented in the collection from left to right in nonincreasing order of their exponents. This is the top row of the Young diagram we are constructing. Then choose the next prime p_2 with the maximal $n(p_2)$ among the remaining primes and write its powers in nonincreasing order of exponents in the second row of the diagram, etc. Since the last invariant factor f_n is divisible by all the previous factors, its prime decomposition consists of the maximal powers of all the primes represented in the collection of elementary divisors, i.e., $f_n = \prod_p p^{m(p)}$ equals the product of elementary divisors in the first column of our Young diagram. Proceeding

¹³Note that the same power p^m can appear several times in the collection of elementary divisors if it appears in the prime factorizations of several of the f_i .

by induction, we conclude that the products of elementary divisors taken along the columns of the Young diagram form a sequence of invariant factors read from right to left. \square

Example 14.7 The following collection of integer elementary divisors,

$$\begin{array}{cccc} 3^2 & 3^2 & 3 & 3 & 3 \\ 2^3 & 2^3 & 2^2 & 2 & \\ 7^2 & 7 & 7 & & \\ 5 & 5 & & & \end{array}$$

appears from the following sequence of invariant factors:

$$f_1 = 3, f_2 = 3 \cdot 2, f_3 = 3 \cdot 2^2 \cdot 7, f_4 = 3^2 \cdot 2^3 \cdot 7 \cdot 5, f_5 = 3^2 \cdot 2^3 \cdot 7^2 \cdot 5.$$

Similarly, looking at the elementary divisors considered before Lemma 14.6,

$$\begin{array}{cccc} 3^3 & 3 & 3 & 3 \\ 2^2 & 2^2 & 2 & 2 \end{array}$$

we recover the initial sequence $6 = 3 \cdot 2$, $6 = 3 \cdot 2$, $12 = 3 \cdot 2^2$, $108 = 3^3 \cdot 2^2$ of invariant factors.

Theorem 14.4 (Elementary Divisors Theorem) *Every finitely generated module M over an arbitrary principal ideal domain K is isomorphic to*

$$K^{n_0} \oplus \frac{K}{(p_1^{n_1})} \oplus \frac{K}{(p_2^{n_2})} \oplus \cdots \oplus \frac{K}{(p_\alpha^{n_\alpha})}, \quad (14.9)$$

where the $p_v \in K$ are irreducible, $m_v \in \mathbb{N}$, and repeated summands are allowed. Two such modules

$$K^{n_0} \oplus \frac{K}{(p_1^{n_1})} \oplus \cdots \oplus \frac{K}{(p_\alpha^{n_\alpha})} \quad \text{and} \quad K^{m_0} \oplus \frac{K}{(q_1^{m_1})} \oplus \cdots \oplus \frac{K}{(q_\beta^{m_\beta})}$$

are isomorphic if and only if $n_0 = m_0$, $\alpha = \beta$, and after appropriate renumbering of the summands we get $n_v = m_v$ and $p_v = s_v q_v$ for some invertible $s_v \in K$.

Definition 14.5 (Elementary Divisors) The decomposition (14.9) for a given finitely generated module M is called the *canonical decomposition*. The collection of (possibly repeated) powers $p_i^{n_i}$ appearing in the canonical decomposition is called the *collection of elementary divisors* of the K -module M . By Theorem 14.4, two K -modules are isomorphic if and only if they have equal collections of elementary divisors and equal free parts K^{n_0} .

We split the proof of Theorem 14.4 into several steps presented in Sects. 14.3.2–14.3.5 below.

14.3.2 Existence of the Canonical Decomposition

Let the vectors w_1, w_2, \dots, w_m span M . Then $M = K^m/R$, where $R \subset K^m$ is the kernel of the K -linear surjection $\pi_w : K^m \twoheadrightarrow M$, which sends the standard basis vector $e_i \in K^m$ to $w_i \in M$. By the invariant factors theorem, Theorem 14.2, there exists a basis u_1, u_2, \dots, u_m in K^m such that some multiples $f_1 u_1, f_2 u_2, \dots, f_k u_k$ of the first $k = \text{rk } R$ vectors form a basis in R . Hence,

$$M = K^m/R = K/(f_1) \oplus \cdots \oplus K/(f_k) \oplus K^{m-k}.$$

For each $f \in \{f_1, f_2, \dots, f_k\}$, consider the prime factorization $f = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$, where all p_i are mutually coprime. By the Chinese remainder theorem,¹⁴

$$K/(f) = K/(p_1^{m_1}) \oplus K/(p_2^{m_2}) \oplus \cdots \oplus K/(p_s^{m_s}).$$

This proves the existence of the decomposition (14.9). To establish its uniqueness, we describe all the direct summands in intrinsic terms of M .

14.3.3 Splitting Off Torsion

The direct sum $K/(p_1^{n_1}) \oplus \cdots \oplus K/(p_\alpha^{n_\alpha})$ in the decomposition (14.9) coincides with the torsion submodule $\text{Tors } M = \{w \in M \mid \exists \lambda \neq 0 : \lambda w = 0\}$, and the number n_0 in (14.9) equals the rank of the free module $M/\text{Tors } M$. Therefore, they do not depend on the particular choice of the decomposition. Note that the existence of the decomposition (14.9) implies the freeness of $M/\text{Tors } M$ and the existence of a free submodule in M complementary to the torsion submodule.

Corollary 14.1 *Every finitely generated module over a principal ideal domain is the direct sum of the torsion submodule and a free module. In particular, every finitely generated torsion-free module over a principal ideal domain is free.* \square

14.3.4 Splitting Off p -Torsion

For each irreducible $p \in K$, we write

$$\text{Tors}_p M \stackrel{\text{def}}{=} \{w \in M \mid \exists k \in \mathbb{N} : p^k w = 0\}$$

¹⁴See Problem 5.8 on p. 120.

for the submodule formed by all vectors annihilated by some power of p . The submodule $\text{Tors}_p M$ is called the p -torsion submodule of M . For every irreducible $q \in K$ not associated¹⁵ with p , multiplication by $p^k : K/(q^m) \rightarrow K/(q^m)$, $x \mapsto p^k x$, is invertible, because p^k is invertible modulo q^m for all m, k . Hence, multiplication by p^k has zero kernel on all summands $K/(q^m)$ with $(q) \neq (p)$. Therefore, the p -torsion submodule $\text{Tors}_p M$ coincides with the direct sum of all components

$$K/(p^\ell), \ell \in \mathbb{N},$$

in the decomposition (14.9). We conclude that this sum does not depend on the particular choice of the decomposition (14.9). The existence of the decomposition (14.9) leads to the following claim.

Corollary 14.2 *Every finitely generated torsion module over a principal ideal domain splits into the direct sum of p -torsion submodules over all irreducible¹⁶ $p \in K$ such that $\text{Tors}_p M \neq 0$. \square*

Exercise 14.20 Write $\varphi_n : K/(p^m) \rightarrow K/(p^m)$, $x \mapsto p^n x$, for the multiplication-by- p^n map. Verify that (a) $\varphi_n = 0$ for $n \geq m$, (b) $\ker \varphi_n = \text{im } \varphi_{m-n} \simeq K/(p^n)$ for $0 < n < m$, (c) $\ker \varphi_n \supset \ker \varphi_{n-1}$ and

$$\ker \varphi_n / \ker \varphi_{n-1} \simeq \begin{cases} 0 & \text{for } n > m, \\ K/(p) & \text{for } 1 \leq n \leq m. \end{cases}$$

14.3.5 Invariance of p -Torsion Exponents

To complete the proof of Theorem 14.4, it remains to verify that for each irreducible $p \in K$ and every K -module M of the form

$$M = \frac{K}{(p^{v_1})} \oplus \cdots \oplus \frac{K}{(p^{v_k})}, \text{ where } v_1 \geq v_2 \geq \cdots \geq v_k,$$

the Young diagram $\nu = (v_1, v_2, \dots, v_k)$ is uniquely determined by M and does not depend on the particular choice of the above decomposition. Write $\varphi_i : M \rightarrow M$, $v \mapsto p^i v$, for the multiplication-by- p^i map. By Exercise 14.20, for each positive integer i , the quotient module $\ker \varphi_i / \ker \varphi_{i-1}$ splits into the direct sum of several copies of $K/(p)$. The total number of these copies is equal to the total number of rows of length $\geq i$ in ν , that is, to the height of the i th column of ν . On the other

¹⁵That is, such that $(q) \neq (p)$, or equivalently, $\text{GCD}(q, p) = 1$ (see Exercise 5.17 on p. 111).

¹⁶Considered up to multiplication by invertible elements.

hand, $\ker \varphi_i / \ker \varphi_{i-1}$ admits a well-defined multiplication by the elements of $K/(p)$, i.e., it is a vector space over the field $K/(p)$.

Exercise 14.21 Verify this.

Thus, the height of the i th column of the diagram ν is equal to

$$\dim_{K/(p)}(\ker \varphi_i / \ker \varphi_{i-1})$$

and therefore does not depend on the choice of decomposition. Hence the diagram ν is uniquely determined by M . This completes the proof of Theorem 14.4.

14.4 Description of Finitely Generated Abelian Groups

14.4.1 Canonical Form of a Finitely Generated Abelian Group

For $K = \mathbb{Z}$, the elementary divisor theorem, Theorem 14.4, provides a complete classification of finitely generated abelian groups.

Theorem 14.5 *Every finitely generated abelian group is isomorphic to a direct product of additive groups*

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \frac{\mathbb{Z}}{(p_2^{n_2})} \oplus \cdots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})}, \quad (14.10)$$

where $p_v, n_i \in \mathbb{N}$, all p_v are prime, and repeated summands are allowed. Two such groups

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \cdots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})} \quad \text{and} \quad \mathbb{Z}^s \oplus \frac{\mathbb{Z}}{(q_1^{m_1})} \oplus \cdots \oplus \frac{\mathbb{Z}}{(q_\beta^{m_\beta})}$$

are isomorphic if and only if $r = s$, $\alpha = \beta$, and after appropriate renumbering of summands, $n_v = m_v$, $p_v = q_v$ for all v . \square

Definition 14.6 The decomposition (14.10) of an abelian group A is called the *canonical form* of A .

Exercise 14.22 For which r, p_v, n_i is the additive abelian group (14.10) cyclic?

In practice, abelian groups typically are described something like, “the abelian group A spanned by the elements a_1, a_2, \dots, a_n constrained by relations

$$\left\{ \begin{array}{l} \mu_{11}a_1 + \mu_{12}a_2 + \cdots + \mu_{1n}a_n = 0, \\ \mu_{21}a_1 + \mu_{22}a_2 + \cdots + \mu_{2n}a_n = 0, \\ \mu_{31}a_1 + \mu_{32}a_2 + \cdots + \mu_{3n}a_n = 0, \\ \quad \dots \\ \mu_{\mu 1}a_1 + \mu_{\mu 2}a_2 + \cdots + \mu_{mn}a_n = 0, \end{array} \right. \quad (14.11)$$

To verify whether a given element $w = x_1a_1 + x_2a_2 + \cdots + x_na_n \in A$ is zero, or more generally, to compute the order¹⁷ $\text{ord}(w)$ in A , Gaussian elimination over \mathbb{Q} can be used as follows. Solve the linear system $w = x_1\mu_1 + x_2\mu_2 + \cdots + x_m\mu_m$ in $x \in \mathbb{Q}^m$. If the system is inconsistent, then w is outside the \mathbb{Q} -linear span of the rows of the matrix (μ_{ij}) . In this case, no integer multiple mw belongs to R , that is, $w \neq 0$ in A and $\text{ord } w = \infty$. If $w = x_1\mu_1 + x_2\mu_2 + \cdots + x_m\mu_m$ for some $x_i = p_i/q_i \in \mathbb{Q}$ such that $\text{GCD}(p_i, q_i) = 1$, then $\text{ord}(w) = \text{LCM}(q_1, q_2, \dots, q_m)$. In particular, $w = 0$ in $A = \mathbb{Z}^n/R$ if and only if all the q_i are equal to 1, that is, the system admits an integer solution $x \in \mathbb{Z}^m$.

Problem 14.1 (Noetherian Modules) Check that the following properties of a module M over an arbitrary commutative ring with unit are equivalent¹⁸:

- (a) Every subset $X \subseteq M$ contains some finite subset $F \subseteq X$ with the same linear span as X .
- (b) Every submodule $N \subseteq M$ is finitely generated.
- (c) For every infinite set of increasing submodules $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ there exists $n \in \mathbb{N}$ such that $N_\nu = N_n$ for all $\nu \geq n$.

¹⁸Modules possessing these properties are called *Noetherian* (compare with Lemma 5.1 on p. 104).

Problem 14.2 Show that a module over a Noetherian ring¹⁹ is Noetherian if and only if it is finitely generated.

Problem 14.3 Show that all submodules and quotient modules of a finitely generated module over a Noetherian ring are finitely generated too.

Problem 14.4 Show that for every module M over an arbitrary commutative ring with unit and every submodule $N \subset M$ such that the quotient module $L = M/N$ is free, we have $M \simeq N \oplus L$.

Problem 14.5 Prove that $\text{Hom}\left(\bigoplus_{\mu=1}^m M_{\mu}, \bigoplus_{v=1}^n N_v\right) = \bigoplus_{\mu,v} \text{Hom}(M_{\mu}, N_v)$.

Problem 14.6 Every \mathbb{Z} -module generated by a single vector is called *cyclic*. Show that:

- (a) Every cyclic \mathbb{Z} -module is isomorphic to either \mathbb{Z} or $\mathbb{Z}/(n)$.
- (b) $\mathbb{Z}/(n) \oplus \mathbb{Z}/(m)$ is cyclic if and only if $\text{GCD}(m, n) = 1$.

Problem 14.7 How many decompositions into a direct sum of two cyclic subgroups does the abelian group $\mathbb{Z}/(5) \oplus \mathbb{Z}/(5)$ admit?

Problem 14.8 How many subgroups of order (a) 2, (b) 6, are there in the noncyclic abelian group of order 12?

Problem 14.9 Show that for every abelian group and a finite set of its finite subgroups of mutually coprime orders, the sum of these subgroups is a direct sum.

Problem 14.10 Given a vector $w = (n_1, n_2, \dots, n_m) \in \mathbb{Z}^n$, show that a \mathbb{Z} -submodule $L \subset \mathbb{Z}^n$ such that $\mathbb{Z}^m = L \oplus \mathbb{Z} \cdot w$ exists if and only if $\text{GCD}(n_1, n_2, \dots, n_m) = 1$. Find such a complementary submodule $L \subset \mathbb{Z}^4$ for $w = (2, 3, 4, 5)$.

Problem 14.11 Is there in \mathbb{Z}^3 a submodule complementary to the \mathbb{Z} -linear span of the vectors (a) $(1, 2, 3)$ and $(4, 5, 6)$? (b) $(1, 2, 2)$ and $(4, 4, 6)$?

Problem 14.12 Write $N \subset \mathbb{Z}[x]$ for the \mathbb{Z} -submodule formed by all polynomials with even constant term. Is it true that N (a) is finitely generated? (b) is free? (c) has a complementary submodule?

Problem 14.13 Enumerate the canonical forms²⁰ of all abelian groups that are semisimple²¹ as \mathbb{Z} -modules.

Problem 14.14 Show that for every finitely generated free \mathbb{Z} -module L and every submodule $N \subset L$ such that L/N is finite, both \mathbb{Z} -modules $L' = \text{Hom}_{\mathbb{Z}}(L, \mathbb{Z})$, $N' = \{\varphi \in \text{Hom}_{\mathbb{Z}}(L, \mathbb{Q}) \mid \varphi(N) \subset \mathbb{Z}\}$ are free and $N'/L' \simeq L/N$.

¹⁹See Sect. 5.1.2 on p. 104.

²⁰See 14.10 on p. 355.

²¹See Sect. 14.1.8 on p. 343.

Problem 14.15 Are the additive groups $\mathbb{Z}/(6) \oplus \mathbb{Z}/(36)$ and $\mathbb{Z}/(12) \oplus \mathbb{Z}/(18)$ isomorphic?

Problem 14.16 Write down the complete list of canonical forms²² of all abelian groups of order 4, 6, 8, 12, 16, 24, 48, 36.

Problem 14.17 How many abelian groups of order 10 000 are there up to isomorphism?

Problem 14.18 Is there in the additive abelian group $\mathbb{Z}/(2) \oplus \mathbb{Z}/(16)$ a subgroup isomorphic to (a) $\mathbb{Z}/(2) \oplus \mathbb{Z}/(8)$? (b) $\mathbb{Z}/(4) \oplus \mathbb{Z}/(4)$? (c) $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$?

Problem 14.19 Write the following abelian groups in canonical form:

- (a) $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/(6), \mathbb{Z}/(12))$,
- (b) $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/(4), \mathbb{Z}/(8))$,
- (c) $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2) \oplus \mathbb{Z}/(2), \mathbb{Z}/(8))$.

Problem 14.20 Show that $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/(m), \mathbb{Z}/(n)) \simeq \mathbb{Z}/(m, n)$.

Problem 14.21 Show that for every field \mathbb{k} ,

- (a) $\text{Hom}_{\mathbb{k}[x]}(\mathbb{k}[x]/(f), \mathbb{k}[x]/(g)) \simeq \mathbb{k}[x]/(f, g)$,
- (a) every $\mathbb{k}[t]$ -linear map $G : \mathbb{k}[t]/(f) \rightarrow \mathbb{k}[t]/(f)$ is a multiplication map $[h] \mapsto [gh]$ by the residue class $[g] = G([1])$.

Problem 14.22 Write in canonical form the quotient group of \mathbb{Z}^3 by the subgroup spanned by:

- (a) $(2, -4, 6), (6, -6, 10), (2, 5, 8), (6, 0, 5)$,
- (b) $(4, 5, 3), (5, 6, 5), (8, 7, 9)$,
- (c) $(-62, -8, -26), (40, 10, 16), (22, -8, 10), (20, 2, 8)$,
- (d) $(7, 2, 3), (21, 8, 9), (5, -4, 3)$,
- (e) $(-81, -6, -33), (60, 6, 24), (-3, 6, -3), (18, 6, 6)$.

Problem 14.23 In the abelian group generated by elements a_1, a_2, a_3 constrained by the relations (a) $a_1 + a_2 + 4a_3 = 2a_1 - a_2 + 2a_3 = 0$, (b) $2a_1 + a_2 - 50a_3 = 4a_1 + 5a_2 + 60a_3 = 0$, find the orders of the elements $a_1 + 2a_3$ and $32a_1 + 31a_3$.

Problem 14.24 Find all integer solutions of the following systems of equations:

$$(a) \begin{cases} x_1 + 2x_2 + 3x_3 + 4x_4 = 0, \\ 4x_1 + 4x_2 + 5x_3 + 5x_4 = 0, \end{cases} \quad (b) \begin{cases} 2x_1 + 2x_2 + 3x_3 + 3x_4 = 0, \\ 4x_1 + 4x_2 + 5x_3 + 5x_4 = 0. \end{cases}$$

Problem 14.25 Write a and b for the residue classes of the unit $1 \in \mathbb{Z}$ in the additive groups $\mathbb{Z}/(9)$ and $\mathbb{Z}/(27)$ respectively. Find the canonical form of the quotient group of $\mathbb{Z}/(9) \oplus \mathbb{Z}/(27)$ by the cyclic subgroup spanned by $3a + 9b$.

²²See Definition 14.6 on p. 355.

Problem 14.26 Let A be a finite abelian group. Show that for every $m \in \mathbb{N}$ dividing $|A|$, there is a subgroup of order m in A .

Problem 14.27 Let some finite abelian groups A, B have the same number of elements of order m for all $m \in \mathbb{N}$. Prove²³ that $A \simeq B$.

Problem 14.28 Show that for every finitely generated modules A, B, C over a principal ideal domain, the isomorphism $A \oplus C \simeq B \oplus C$ implies the isomorphism $A \simeq B$.

Problem 14.29 Show that for every integer $n \geq 3$, the multiplicative group of invertible elements in the residue class ring $\mathbb{Z}/(2^n)$ is isomorphic to the additive group $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2^{n-2})$.

Problem 14.30 (Integer-valued Polynomials) Write

$$M \stackrel{\text{def}}{=} \{f \in \mathbb{Q}[x] \mid \forall m \in \mathbb{Z} f(m) \in \mathbb{Z}\}$$

for the \mathbb{Z} -module of *integer-valued* polynomials with rational coefficients and let $M_d \subset M$ be the submodule formed by the polynomials of degree at most d . Verify that the polynomials $\gamma_0 \stackrel{\text{def}}{=} 1$ and

$$\gamma_k(x) = \binom{x+d}{d} = \frac{1}{d!}(x+1)(x+2)\cdots(x+d), \quad 1 \leq k \leq d,$$

form a basis of M_d over \mathbb{Z} and find the cardinality of the quotient module

$$M_d/(M_d \cap \mathbb{Z}[x]).$$

Show that for every \mathbb{Z} -linear map $F : M \rightarrow M$ commuting with the shift $f(x) \mapsto f(x+1)$, there exists a unique power series $f \in \mathbb{Z}[[t]]$ such that $F = f(\nabla)$, where $\nabla : f(x) \mapsto f(x) - f(x-1)$.

Problem 14.31 (Rank of a Matrix over a Principal Ideal Domain) Let K be an arbitrary principal ideal domain. Show that for every matrix $M \in \text{Mat}_{m \times n}(K)$, the submodules generated within K^m and K^n by the rows and columns of M are free of the same rank equal to the number of nonzero elements in the Smith normal form of M .

Problem 14.32 (Pick's Formula for Parallelepipeds) For a triple of integer vectors $v_1, v_2, v_3 \in \mathbb{Z}^3 \subset \mathbb{R}^3$ linearly independent over \mathbb{R} , write $L \subset \mathbb{Z}^3$ and $\Pi \subset \mathbb{R}^3$ for the \mathbb{Z} -submodule and the real parallelepiped spanned by these

²³Compare with [Problem 12.11](#) on p. 304.

vectors. Show that the Euclidean volume of Π equals the cardinality of the quotient group \mathbb{Z}^3/L and that it can be computed as $v + f/2 + e/4 + 1$, where v, f, e denote the numbers of internal integer points²⁴ within Π , faces of Π , and edges of Π respectively. Extend both claims to higher dimensions.

Problem 14.33 Is there a matrix $Z \in \text{Mat}_3(\mathbb{Z})$ such that $Z^2 = \begin{pmatrix} 4 & -5 & 7 \\ 1 & -4 & 9 \\ -4 & 0 & 5 \end{pmatrix}$?

²⁴That is, points with integer coordinates lying inside but not on the boundary of Π , faces of Π , and edges of Π respectively.

Chapter 15

Linear Operators

15.1 Classification of Operators

15.1.1 Spaces with Operators

Let \mathbb{k} be an arbitrary field, V a finite-dimensional vector space over \mathbb{k} , and $F : V \rightarrow V$ a linear endomorphism of V over \mathbb{k} . We call a pair (F, V) a *space with operator* or just an *operator* over \mathbb{k} . Given two spaces with operators (F_1, U_1) and (F_2, U_2) , a linear map $C : U_1 \rightarrow U_2$ is called a *homomorphism* of spaces with operators if $F_2 \circ C = C \circ F_1$, or equivalently, if the diagram of linear maps

$$\begin{array}{ccc} U_1 & \xrightarrow{C} & U_2 \\ F_1 \uparrow & & \uparrow F_2 \\ U_1 & \xrightarrow{C} & U_2 \end{array}$$

is commutative.¹ If C is an isomorphism of vector spaces, the operators F_1 and F_2 are called *similar* or *isomorphic*. In this case, $F_2 = CF_1C^{-1}$, and we also say that F_2 is *conjugate* to F_1 by C .

15.1.2 Invariant Subspaces and Decomposability

Let (F, V) be a space with operator. A subspace $U \subset V$ is called *F-invariant* if $F(U) \subset U$. In this case, $(F|_U, U)$ is also a space with operator, and the inclusion $U \hookrightarrow V$ is a homomorphism of spaces with operators. If F has no invariant

¹See [Problem 7.7](#) on p. 168.

subspaces except for zero and the whole space, we say that F is *irreducible* or *simple*.

Exercise 15.1 Check that multiplication by a residue class $[t]$ in the quotient ring $\mathbb{R}[t]/(t^2 + 1)$ is irreducible over \mathbb{R} .

An operator $F : V \rightarrow V$ is called *decomposable* if $V = U \oplus W$, where both subspaces $U, W \subset V$ are nonzero and F -invariant. Otherwise, F is called *indecomposable*. For example, all irreducible operators are indecomposable. Every space with operator clearly can be split into a direct sum of indecomposable invariant subspaces. The next exercise shows that over any field \mathbb{k} , there are indecomposable operators of every dimension, and not all such operators are irreducible.

Exercise 15.2 Check that multiplication by a residue class $[t]$ in the quotient ring $\mathbb{k}[t]/(t^n)$ is indecomposable for all n and is irreducible if and only if $n = 1$.

Exercise 15.3 Show that the dual operators² $F : V \rightarrow V$ and $F^* : V^* \rightarrow V^*$ are either both decomposable or both indecomposable.

15.1.3 Space with Operator as a $\mathbb{k}[t]$ -Module

Every linear operator $F : V \rightarrow V$ provides V with the structure of a $\mathbb{k}[t]$ -module in which multiplication of a vector $v \in V$ by a polynomial

$$f(t) = a_0 + a_1 t + \cdots + a_m t^m \in \mathbb{k}[t]$$

is defined by $f \cdot v \stackrel{\text{def}}{=} f(F)v = a_0 v + a_1 Fv + a_2 F^2 v + \cdots + a_m F^m v$. We denote this $\mathbb{k}[t]$ -module by V_F and say that it is *associated* with F . Every $\mathbb{k}[t]$ -module structure on V is associated with a linear operator $t : V \rightarrow V$, $v \mapsto t \cdot v$, provided by the multiplication of vectors by t in this structure. Therefore, a space with operator and a $\mathbb{k}[t]$ -module of finite dimension over \mathbb{k} are the same thing.

A homomorphism $C : V_F \rightarrow W_G$ of $\mathbb{k}[t]$ -modules associated with operators $F : V \rightarrow V$ and $G : W \rightarrow W$ is nothing but a \mathbb{k} -linear map $C : V \rightarrow W$ commuting with the multiplication of vectors by t , i.e., such that $C \circ F = G \circ C$. In particular, $\mathbb{k}[t]$ -modules V_F and W_G are isomorphic if and only if the operators F and G are similar. A vector subspace $U \subset V$ is a $\mathbb{k}[t]$ -submodule of the $\mathbb{k}[t]$ -module V_F if and only if multiplication by t takes U to itself, that is, exactly when U is F -invariant. The decomposition of V into a direct sum of F -invariant subspaces means the same as the decomposition of the $\mathbb{k}[t]$ -module V_F into a direct sum of $\mathbb{k}[t]$ -submodules. In other words, the structure theory of operators is identical to the structure theory of $\mathbb{k}[t]$ -modules finite-dimensional over \mathbb{k} .

²See Sect. 7.3 on p. 164.

Theorem 15.1 *Each linear operator on a finite-dimensional vector space over an arbitrary field \mathbb{k} is similar to multiplication by t in a direct sum of residue modules*

$$\frac{\mathbb{k}[t]}{(p_1^{m_1})} \oplus \cdots \oplus \frac{\mathbb{k}[t]}{(p_k^{m_k})}, \quad (15.1)$$

where all $p_v \in \mathbb{k}[t]$ are monic irreducible polynomials, and repeated summands are allowed. Two multiplication-by- t operators acting on the direct sums

$$\frac{\mathbb{k}[t]}{(p_i^{m_i})} \oplus \cdots \oplus \frac{\mathbb{k}[t]}{(p_k^{m_k})} \quad \text{and} \quad \frac{\mathbb{k}[t]}{(q_i^{n_i})} \oplus \cdots \oplus \frac{\mathbb{k}[t]}{(q_\ell^{n_\ell})}$$

are similar if and only if $k = \ell$ and after appropriate renumbering we get $p_v = q_v$, $m_v = n_v$ for all v . All direct summands in (15.1) are indecomposable.

Proof By the elementary divisors theorem, Theorem 14.4 on p. 352, the $\mathbb{k}[t]$ -module V_F associated with a arbitrary operator $F : V \rightarrow V$ is a direct sum of a free module $\mathbb{k}[t]^m$ and a torsion module of the form (15.1). Since $\mathbb{k}[t]^m$ is infinite-dimensional as a vector space over \mathbb{k} for $m > 0$, the free component of V_F vanishes. Now the first two statements of Theorem 15.1 follow immediately from Theorem 14.4. The last statement is also a part of Theorem 14.4, because the decomposability of the $\mathbb{k}[t]$ -module $\mathbb{k}[t]/(p^m)$, where $p \in \mathbb{k}[t]$ is a monic irreducible polynomial, contradicts the uniqueness of the decomposition (15.1) written for $\mathbb{k}[t]/(p^m)$ itself. \square

Corollary 15.1 *Each indecomposable operator is similar to multiplication by t in the residue module $\mathbb{k}[t]/(p^m)$, where $p \in \mathbb{k}[t]$ is monic irreducible. Such an operator is irreducible if and only if $m = 1$. Two indecomposable operators acting on $\mathbb{k}[t]/(p^m)$ and $\mathbb{k}[t]/(q^n)$ are similar if and only if $p = q$ and $m = n$.*

Proof The first and third statements are contained in Theorem 15.1. Let us prove the second. Every $\mathbb{k}[t]$ -submodule in $\mathbb{k}[t]/(p^m)$ is an ideal of this quotient ring. For $m = 1$, the residue ring $\mathbb{k}[t]/(p)$ is a field³ and therefore has no nontrivial ideals.⁴ For $m \geq 2$, the principal ideal spanned by the class $[p] = p \pmod{p^m}$ is proper. \square

15.1.4 Elementary Divisors

The unordered disjoint collection of all polynomials $p_v^{m_v}$ appearing in the decomposition (15.1) is called the *collection of elementary divisors* of the operator $F : V \rightarrow V$ and is denoted by $\mathcal{E}\ell(F)$. Note that it may contain several copies of the same polynomial p^m , which occurs in $\mathcal{E}\ell(F)$ as many times as there are

³See Proposition 3.8 on p. 53.

⁴See Proposition 5.1 on p. 103.

summands $\mathbb{k}[t]/(p^m)$ in the decomposition (15.1). A straightforward conclusion from Theorem 15.1 is the following corollary.

Corollary 15.2 *Two linear operators F and G are similar if and only if $\mathcal{E}(F) = \mathcal{E}(G)$.* \square

Exercise 15.4 Let a space with operator F split into the direct sum of F -invariant subspaces U_i on which F is restricted to operators $F_i : U_i \rightarrow U_i$. Show that $\mathcal{E}(F) = \bigsqcup \mathcal{E}(F_i)$.

Practical computation of elementary divisors for a given operator $F : V \rightarrow V$ can be done as follows. Choose a basis $\mathbf{v} = (v_1, v_2, \dots, v_n)$ in V and write $F_{\mathbf{v}} \in \text{Mat}_n(\mathbb{k})$ for the matrix of F in this basis. We will see instantly that the collection of elementary divisors $\mathcal{E}(F)$ is associated with a sequence of invariant factors⁵ f_1, f_2, \dots, f_n of the matrix $tE - F_{\mathbf{v}} \in \text{Mat}_n(\mathbb{k}[t])$ over $\mathbb{k}[t]$. Therefore, to get $\mathcal{E}(F)$, we first compute the invariant factors f_i of the matrix $tE - F_{\mathbf{v}}$ either as diagonal elements of its Smith form⁶ or by the formula $f_k = \Delta_k(tE - F_{\mathbf{v}}) / \Delta_{k-1}(tE - F_{\mathbf{v}})$, where Δ_k means the GCD of all $k \times k$ minors, then realize the irreducible factorization $f_i = p_{i1}^{m_{i1}} p_{i2}^{m_{i2}} \cdots p_{ik_i}^{m_{ik_i}}$ of each factor, then collect disjointly all factors p^m appearing in these factorizations. The coincidence of $\mathcal{E}(F)$ with the collection of elementary divisors of the matrix $tE - F_{\mathbf{v}} \in \text{Mat}_n(\mathbb{k}[t])$ follows immediately from the following description of the $\mathbb{k}[t]$ -module V_F by generators and relations. The basis vectors v_i , which span V_F even over \mathbb{k} , certainly generate V_F over $\mathbb{k}[t]$. Therefore, we have an epimorphism of $\mathbb{k}[t]$ -modules $\pi_{\mathbf{v}} : \mathbb{k}[t]^n \rightarrow V_F$ sending the standard basis vector $e_i \in \mathbb{k}[t]^n$ to v_i . Hence, $V_F \simeq \mathbb{k}[t]^n / \ker \pi$.

Lemma 15.1 *Write the elements of $\mathbb{k}[t]^n$ as coordinate columns with elements in $\mathbb{k}[t]$. Then the relation submodule $\ker \pi_{\mathbf{v}} \subset \mathbb{k}[t]^n$ is spanned over $\mathbb{k}[t]$ by the columns of the matrix $tE - F_{\mathbf{v}}$.*

Proof Let $F_{\mathbf{v}} = (f_{ij})$. Then the j th column of $tE - F_{\mathbf{v}}$ is expressed through the standard basis \mathbf{e} as $te_j - f_{1j}e_1 - f_{2j}e_2 - \cdots - f_{nj}e_n$. When we apply $\pi_{\mathbf{v}}$ to this vector, we get

$$\pi_{\mathbf{v}} \left(te_j - \sum_{i=1}^n e_i f_{ij} \right) = tv_j - \sum_{i=1}^n v_i f_{ij} = Fv_j - \sum_{i=1}^n v_i f_{ij} = 0.$$

Thus, all columns of $tE - F_{\mathbf{v}}$ lie in $\ker \pi_{\mathbf{v}}$. Every vector $h \in \mathbb{k}[t]^n$ can be written as

$$h = t^m h_m + t^{m-1} h_{m-1} + \cdots + th_1 + h_0, \quad (15.2)$$

⁵See Sect. 14.3 on p. 351.

⁶See Definition 14.4 on p. 345.

where the coefficients $h_i \in \mathbb{K}^n$ are columns of scalar constants. The same long-division process⁷ as for ordinary polynomials with constant coefficients allows us to divide the polynomial (15.2) from the left side by the polynomial $tE - F_v$ with remainder of degree zero in t , i.e.,

$$t^m h_m + \cdots + t h_1 + h_0 = (tE - F_v) \cdot (t^{m-1} g_{m-1} + \cdots + t g_1 + g_0) + r \quad (15.3)$$

for appropriate $g_i, r \in \mathbb{K}^n$.

Exercise 15.5 Convince yourself of this.

It follows from (15.3) that every vector $h \in \mathbb{K}[t]^n$ can be written as $h = (tE - F_v)g + r$ for appropriate $g \in \mathbb{K}[t]^n$ and $r \in \mathbb{K}^n$. In other words, each column in $\mathbb{K}[t]^n$ is congruent modulo the columns of the matrix $tE - F_v$ to a column of constants, that is, to some linear combination $\sum \lambda_i e_i$, where $\lambda_i \in \mathbb{K}$. In particular, $\pi_v(h) = \sum \lambda_i v_i$. If $h \in \ker(\pi_v)$, then the latter sum is zero. This forces all λ_i to equal 0, because the v_i form a basis in V . Hence, all $h \in \ker \pi_v$ lie in the linear span of the columns of the matrix $tE - F_v$. \square

Exercise 15.6 Show that dual operators⁸ $F : V \rightarrow V$ and $F^* : V^* \rightarrow V^*$ are similar over every field. (Equivalently, every square matrix A is conjugate to the transposed matrix A' .)

15.1.5 Minimal Polynomial

For a monic irreducible polynomial $p \in \mathbb{K}[t]$, we write $m_p(F)$ for the maximal integer m such that $p^m \in \mathcal{E}\ell(F)$. Therefore, $m_p(F) = 0$ for all p except those appearing in (15.1). We call $m_p(F)$ the *index* of p in $\mathcal{E}\ell(F)$. It follows from Theorem 15.1 that the *minimal polynomial*⁹ of F is equal to

$$\mu_F(t) = \prod_p p^{m_p(F)},$$

which is the least common multiple of all elementary divisors.

Corollary 15.3 A polynomial $f \in \mathbb{K}[t]$ annihilates an operator $F : V \rightarrow V$ if and only if f is divisible by each elementary divisor of F . \square

⁷See Sect. 3.2 on p. 46.

⁸See Sect. 7.3 on p. 164.

⁹That is, the monic polynomial $\mu_F(t)$ of lowest positive degree such that $\mu_F(F) = 0$ (see Sect. 8.1.3 on p. 175).

15.1.6 Characteristic Polynomial

Let F_v be the matrix of the operator $F : V \rightarrow V$ in some basis v of V . The characteristic polynomial of this matrix $\chi_{F_v}(t) = \det(tE - F_v)$ does not depend on the choice of basis, because in another basis $w = vC$, we get¹⁰ $F_w = C^{-1}F_vC$ and

$$\begin{aligned}\det(tE - F_w) &= \det(tE - C^{-1}F_vC) = \det(C^{-1}(tE - F_v)C) \\ &= \det C^{-1} \cdot \det(tE - F_v) \cdot \det C = \det(tE - F_v) .\end{aligned}$$

For this reason, $\chi_F(t) \stackrel{\text{def}}{=} \det(tE - F_v)$ is called the characteristic polynomial of the operator F . The previous computation shows that similar operators have equal characteristic polynomials.

Exercise 15.7 Let an operator F be decomposable as the direct sum of operators G, H . Check that $\chi_F(t) = \chi_G(t) \cdot \chi_H(t)$.

Exercise 15.8 For a monic polynomial $f \in \mathbb{k}[t]$, check that the characteristic polynomial of the multiplication-by- t operator in the residue class module $\mathbb{k}[t]/(f)$ equals f .

These exercises together with Theorem 15.1 lead to the following result.

Corollary 15.4 *The characteristic polynomial of an operator F is the product of all the elementary divisors of F .* \square

Exercise 15.9 Use Corollary 15.4 to give a new proof of the Cayley–Hamilton identity.¹¹

Proposition 15.1 *Every operator F over a field \mathbb{R} has an invariant subspace of dimension ≤ 2 .*

Proof Let the characteristic polynomial of F be factored as $\chi_F = q_1 \cdot q_2 \cdots q_m$, where $q_i \in \mathbb{R}[t]$ are monic irreducible polynomials, not necessarily distinct. Note that $\deg q_i \leq 2$ for each i . If we apply the zero operator $0 = \chi_F(F) = q_1(F) \circ q_2(F) \circ \cdots \circ q_m(F)$ to any nonzero vector $v \in V$, then for some $i \geq 0$, we obtain a nonzero vector $w = q_{i+1}(F) \circ \cdots \circ q_m(F) v \neq 0$ such that $q_i(F)w = 0$. If $q_i(t) = t - \lambda$ is linear, then $F(w) = \lambda w$, and we get a 1-dimensional invariant subspace $\mathbb{k} \cdot w$. If $q_i(t) = t^2 - \alpha t - \beta$ is quadratic, then $F(Fw) = \alpha F(w) + \beta w$ remains within the linear span of w, Fw , and we get at most a 2-dimensional F -invariant subspace generated by w and Fw . \square

¹⁰See formula (8.13) on p. 182.

¹¹Which says that $\chi_F(F) = 0$.

Corollary 15.5 (From the Proof of Proposition 15.1) *Every linear operator over an arbitrary algebraically closed field has an invariant subspace of dimension one.*

□

15.2 Operators of Special Types

In this section we discuss some particular types of operators: nilpotent, semisimple, cyclic, and diagonalizable. All these types play important special roles in many branches of mathematics as well as in applications. We characterize operators of each type in two ways: as $\mathbb{k}[t]$ -modules and in intrinsic terms concerned with their action on V .

15.2.1 Nilpotent Operators

An operator $F : V \rightarrow V$ is called *nilpotent* if $F^m = 0$ for some $m \in \mathbb{N}$. Let F be nilpotent. Since F is annihilated by a polynomial t^m , all elementary divisors of F have the form t^{ν} , i.e., F is similar to multiplication by t in the direct sum of residue class modules

$$\frac{\mathbb{k}[t]}{(t^{\nu_1})} \oplus \cdots \oplus \frac{\mathbb{k}[t]}{(t^{\nu_k})}. \quad (15.4)$$

Let us number the exponents in nonincreasing order $\nu_1 \geq \nu_2 \geq \cdots \geq \nu_k$. By Theorem 15.1, this nonincreasing sequence of positive integers determines F uniquely up to conjugation. In other words, the conjugation classes of nilpotent operators over a field \mathbb{k} are in bijection with the Young diagrams. The Young diagram $\nu(F)$ corresponding to a nilpotent operator F is called the *cyclic type* of F .

Write $[f]$ for the residue class $f \pmod{t^m}$ and choose

$$e_1 = [t^{m-1}], e_2 = [t^{m-2}], \dots, e_m = [1]$$

as a basis in $\mathbb{k}[t]/(t^m)$. Multiplication by t acts as

$$0 \leftarrow e_1 \leftarrow e_2 \leftarrow e_3 \leftarrow \cdots \leftarrow e_{m-1} \leftarrow e_m,$$

that is, has matrix

$$J_m(0) \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

This matrix is called a *nilpotent Jordan block* of size m . Thus, a nilpotent operator F of cyclic type ν admits a basis whose vectors can be written in the cells of a diagram ν in such a way that F annihilates the leftmost vector of each row and sends every other vector to its left neighbor, as in the following example:

$$\begin{array}{c} \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \end{array} \quad \longleftrightarrow \quad \begin{array}{l} 0 \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \\ 0 \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \\ 0 \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \\ 0 \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \\ 0 \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \end{array} \quad (15.5)$$

A basis of this type is called a *Jordan basis*.¹² The elements of such a basis are combined in sequences along the rows of the Young diagram. These sequences are called *Jordan chains*.

The cyclic type of F can be determined in terms of the action of F on V as follows. The total number of cells in the leftmost m columns of the diagram $\nu(F)$ is equal to $\dim \ker F^m$. Thus, the m th column of the diagram $\nu(F)$ has length¹³

$$\nu_m^t(F) = \dim \ker F^m - \dim \ker F^{m-1}. \quad (15.6)$$

15.2.2 Semisimple Operators

An operator $F : V \rightarrow V$ is called *semisimple*¹⁴ if V is a direct sum of simple (or irreducible) spaces with operators. Semisimplicity is somehow “complementary” to nilpotency. It has several equivalent characterizations.

Proposition 15.2 *The following properties of an operator $F : V \rightarrow V$ are equivalent:*

- (1) V is a direct sum of irreducible F -invariant subspaces.
- (2) V is linearly generated by irreducible F -invariant subspaces.
- (3) For every proper F -invariant subspace $U \subset V$, there exists an F -invariant subspace $W \subset V$ such that $V = U \oplus W$.
- (4) F is similar to multiplication by t in the direct sum of residue modules

$$\mathbb{k}[t]/(p_1) \oplus \mathbb{k}[t]/(p_2) \oplus \cdots \oplus \mathbb{k}[t]/(p_r),$$

where $p_i \in \mathbb{k}[t]$ are monic irreducible, and repeated summands are allowed (in other words, all exponents $m_i = 1$ in formula (15.1) on p. 363).

¹²Or cyclic basis.

¹³Recall that we write ν_i for the length of the i th row in the Young diagram ν and write ν^t for the transposed Young diagram. Thus, ν_m^t means the length of the m th column of ν .

¹⁴Or completely reducible.

Proof The implication (1) \Rightarrow (2) is obvious. Let us prove the implication (2) \Rightarrow (3). For every irreducible F -invariant subspace $L \subset V$, the intersection $L \cap U$ is either zero or L , because $L \cap U \subset L$ is F -invariant. If U contains all F -invariant irreducible subspaces of V , then $U = V$ by (2). Since U is proper, there exists a nonzero irreducible F -invariant subspace $L \subset V$ such that $L \cap U = 0$. If $U \oplus L = V$, we are done. If not, we replace U by $U' = U \oplus L$ and repeat the argument. Since $\dim U' > \dim U$, after a finite number of steps we will have constructed a sequence of nonzero irreducible F -invariant subspaces L_1, L_2, \dots, L_k such that $L_1 = L$, $L_i \cap (U \oplus L_1 \oplus L_2 \oplus \dots \oplus L_{i-1}) = 0$ for $1 \leq i \leq k$, and $U \oplus L_1 \oplus L_2 \oplus \dots \oplus L_k = V$. Then $W = L_1 \oplus L_2 \oplus \dots \oplus L_k$ is what we need.

To verify the implication (3) \Rightarrow (4), let us show first that if (3) holds in V , then (3) holds in every F -invariant subspace $H \subset V$. Consider a proper F -invariant subspace $U \subset H$. There exist F -invariant subspaces $Q, R \subset V$ such that $V = H \oplus Q = U \oplus Q \oplus R$. Write $\pi : V \rightarrow H$ for the projection along Q and put $W = \pi(R)$.

Exercise 15.10 Check that $H = U \oplus W$.

Thus, if (3) is true for a direct sum (15.1), then (3) holds within each direct summand. By Corollary 15.1, all summands $\mathbb{k}[t]/(p^m)$ are indecomposable. However, if $m > 1$, then $\mathbb{k}[t]/(p^m)$ contains some proper invariant subspaces. Hence, if (3) holds in V , then all exponents m_i are equal to 1 in the decomposition (15.1). The implication (4) \Rightarrow (1) follows immediately from Corollary 15.1. \square

Corollary 15.6 (From the Proof of Proposition 15.2) *The restriction of a semisimple operator F onto any F -invariant subspace is semisimple.*

Example 15.1 (Euclidean Isometries) Let us show that every orthogonal operator¹⁵ $F : V \rightarrow V$ on a Euclidean vector space V is semisimple. For every proper F -invariant subspace $U \subset V$, there is an orthogonal decomposition¹⁶ $V = U \oplus U^\perp$. Let us verify that the orthogonal complement U^\perp is F -invariant. Since the restriction $F|_U$ is a Euclidean isometry of U , it is bijective, and therefore for each $u \in U$, there is $u' \in U$ such that $u = Fu'$. Hence for each $w \in U^\perp$ and $u \in U$, we have $(Fw, u) = (Fw, Fu') = (w, u') = 0$, that is, $Fw \in U^\perp$, as required. We know from Proposition 15.1 on p. 366 that every operator on a real vector space F has a 1- or 2-dimensional invariant subspace. For every semisimple operator F , such an invariant space splits off as a direct summand. The previous argument shows that for a Euclidean isometry, it is an *orthogonal* direct summand. We conclude that a Euclidean vector space with isometry F splits into an orthogonal direct sum of 1-dimensional subspaces, where F acts as $\pm \text{Id}$, and 2-dimensional subspaces, where F acts as rotation.

Exercise 15.11 Deduce the last statement from Example 10.10 and Example 10.11 on p. 245.

¹⁵See Sect. 10.5 on p. 244.

¹⁶See Sect. 10.1 on p. 237.

Theorem 15.2 (Normal Form of a Euclidean Isometry) *For every Euclidean isometry $F : V \rightarrow V$, there exists an orthonormal basis of V in which F has a block-diagonal matrix formed by one-cell blocks ± 1 and 2×2 blocks*

$$\begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}, \text{ where } 0 < \varphi < \pi,$$

representing counterclockwise rotation about the origin by the angle $\varphi \in (0, \pi)$. Up to a permutation of blocks, this block-diagonal matrix does not depend on the choice of the orthonormal basis in question.

Proof The existence was explained in Example 15.1. To see uniqueness, note that each 1-dimensional isometry $\pm \text{Id}$ contributes an elementary divisor $t \mp 1$ to $\mathcal{E}(F)$, and each rotation of the plane by the angle φ contributes an elementary divisor $t^2 - 2 \cos \varphi \cdot t + 1$ to $\mathcal{E}(F)$. Thus, the blocks are in bijection with the elementary divisors of F . \square

15.2.3 Cyclic Vectors and Cyclic Operators

A vector $v \in V$ is called a *cyclic vector* of the linear operator $F : V \rightarrow V$ if its F -orbit v, Fv, F^2v, F^3v, \dots spans V over \mathbb{k} , or equivalently, if v generates V_F over $\mathbb{k}[t]$. Operators possessing cyclic vectors are called *cyclic*.

Proposition 15.3 *The following properties of an operator $F : V \rightarrow V$ are equivalent:*

- (1) F is cyclic.
- (2) F is similar to multiplication by t in the residue class module $\mathbb{k}[t]/(f)$, where $f \in \mathbb{k}[t]$ is an arbitrary monic polynomial.
- (3) Each monic irreducible $p \in \mathbb{k}[t]$ appears in $\mathcal{E} F$ at most once.
- (4) The minimal and characteristic polynomials of F coincide.

Proof The equivalence (3) \iff (4) follows at once from Corollary 15.4. Both conditions mean that F is similar to multiplication by t in the direct sum of residue class modules

$$\mathbb{k}[t]/(p_1^{m_1}) \oplus \mathbb{k}[t]/(p_2^{m_2}) \oplus \dots \oplus \mathbb{k}[t]/(p_r^{m_r}),$$

where p_1, p_2, \dots, p_r are monic, irreducible, and distinct. By the Chinese remainder theorem, this sum is isomorphic to the residue class module $\mathbb{k}[t]/(f)$, where

$$f = \chi_F = \mu_F = \prod_{i=1}^r p_i^{m_i}.$$

Thus, (2) is equivalent to (3), (4). The implication (2) \Rightarrow (1) is obvious: the class of the unit $[1]$ is a cyclic vector for multiplication by t in $\mathbb{k}[t]/(f)$. Conversely, if V_F is generated by v over $\mathbb{k}[t]$, then a $\mathbb{k}[t]$ -linear surjection $\pi : \mathbb{k}[t] \twoheadrightarrow V_F$ is given by $1 \mapsto v$. Hence, $V_F = \mathbb{k}[t]/\ker \pi$. Since $\mathbb{k}[t]$ is a principal ideal domain, the ideal $\ker \pi \subset \mathbb{k}[t]$ has the form (f) for some monic $f \in \mathbb{k}[t]$. Thus, (1) \Rightarrow (2). \square

Exercise 15.12 Show that multiplication-by- t operators in $\mathbb{k}[t]/(f)$ and $\mathbb{k}[t]/(g)$ (where f, g both are monic) are similar if and only if $f = g$.

15.2.4 Eigenvectors and Eigenvalues

A nonzero vector $v \in V$ is called an *eigenvector* of an operator $F : V \rightarrow V$ if $F(v) = \lambda v$ for some $\lambda \in \mathbb{k}$. In this case, λ is called an *eigenvalue* of F . The set of all eigenvalues is called the *spectrum* of F in \mathbb{k} and is denoted by

$$\text{Spec}_{\mathbb{k}}(F) = \{\lambda \in \mathbb{k} \mid \exists v \in V \setminus 0 : Fv = \lambda v\}$$

(we will omit the index \mathbb{k} when it is not important). Note that $\text{Spec}_{\mathbb{k}}(F)$ is a subset of \mathbb{k} , and each $\lambda \in \text{Spec}(F)$ is counted there just once (in contrast with $\mathcal{E}\ell(F)$, where we allow multiple entries).

Proposition 15.4 $\text{Spec}_{\mathbb{k}}(F)$ coincides with the set of roots¹⁷ of the characteristic polynomial $\chi_F(t) = \det(t \text{Id} - F)$ in \mathbb{k} . In particular, $|\text{Spec}(F)| \leq \dim V$.

Proof An eigenvector v with eigenvalue λ lies in the kernel of the linear operator $\lambda \text{Id} - F$. By Corollary Exercise 9.12, $\ker(\lambda E - F) \neq 0$ if and only if $\det(\lambda \text{Id} - F) = 0$. \square

Corollary 15.7 If \mathbb{k} is algebraically closed, then $\text{Spec}_{\mathbb{k}}(F) \neq \emptyset$ for every operator F . In particular, every operator has an eigenvector.¹⁸ \square

Exercise 15.13 Prove that over every field \mathbb{k} the spectrum $\text{Spec}_{\mathbb{k}} F$ is contained in the set of roots of every polynomial $f \in \mathbb{k}[t]$ such that $f(F) = 0$.

Exercise 15.14 Prove that over an algebraically closed field \mathbb{k} , an operator F is nilpotent if and only if $\text{Spec}_{\mathbb{k}} F = \{0\}$.

Proposition 15.5 Every set of eigenvectors with distinct eigenvalues is linearly independent.

¹⁷Counted without multiplicities.

¹⁸Note that this agrees with Corollary 15.5 on p. 367.

Proof Assume the contrary and let $x_1v_1 + x_2v_2 + \cdots + x_kv_k = 0$ be a linear relation of minimal length k . Write $\lambda_1, \lambda_2, \dots, \lambda_k$ for the eigenvalues of v_1, v_2, \dots, v_m respectively. If we apply the operator to the previous relation, then we get another relation, $x_1\lambda_1v_1 + x_2\lambda_2v_2 + \cdots + x_k\lambda_kv_k = 0$. Multiply the first relation by λ_k and subtract from the second. We get a strictly shorter relation

$$0 = x_1(\lambda_1 - \lambda_k) \cdot v_1 + x_2(\lambda_2 - \lambda_k) \cdot v_2 + \cdots + x_{k-1}(\lambda_{k-1} - \lambda_k) \cdot v_{k-1}$$

with nonzero coefficients. Contradiction. \square

15.2.5 Eigenspaces

For each $\lambda \in \mathbb{k}$, a subspace $V_\lambda \stackrel{\text{def}}{=} \{v \in V \mid F(v) = \lambda v\} = \ker(\lambda \text{Id}_V - F)$ is called a λ -eigenspace of F . It is nonzero if and only if $\lambda \in \text{Spec}(F)$, or equivalently, $\chi_F(\lambda) = 0$. Each eigenspace V_λ is F -invariant, and $F|_{V_\lambda} = \lambda \cdot \text{Id}_{V_\lambda}$. From Proposition 15.5, we get the following corollary.

Corollary 15.8 *A sum of nonzero eigenspaces is a direct sum, and $\sum_{\lambda \in \text{Spec } F} \dim V_\lambda \leq \dim V$.* \square

Exercise 15.15 Give an example of a linear operator for which the inequality is strict.

15.2.6 Diagonalizable Operators

A linear operator $F : V \rightarrow V$ is called *diagonalizable* if it has a diagonal matrix in some basis of V . Such a basis consists of eigenvectors of F , and the elements of the diagonal matrix are the eigenvalues of F . The characteristic polynomial $\chi_F(t) = \det(tE - F)$ computed by means of such a diagonal matrix is the product $\prod_\lambda (t - \lambda)$, where λ runs through the diagonal elements. We conclude that each $\lambda \in \text{Spec}(F)$ appears on the diagonal, and the number of its appearances is equal to both $\dim V_\lambda$ and the multiplicity of the root λ in $\chi_F(t)$. Thus, up to a permutation of the diagonal elements, a diagonal matrix of F does not depend on the choice of basis in which F has a diagonal matrix. From the $\mathbb{k}[t]$ -module viewpoint, we can say that a diagonalizable operator F is similar to multiplication by t in a direct sum of residue modules $\mathbb{k}[t]/(t - \lambda) \simeq \mathbb{k}$, where λ runs through $\text{Spec } F$ and every such summand appears in the direct sum exactly $\dim V_\lambda$ times.

Proposition 15.6 *The following properties of a linear operator $F : V \rightarrow V$ are equivalent:*

- (1) F is diagonalizable.
- (2) V is spanned by the eigenvectors of F .
- (3) The characteristic polynomial $\chi_F(t) = \det(tE - F)$ is completely factorizable in $\mathbb{k}[t]$ into a product of linear factors, and the multiplicity of each factor $(t - \lambda)$ is equal to $\dim V_\lambda$.
- (4) All elementary divisors of F have the form $(t - \lambda)$, where $\lambda \in \mathbb{k}$.
- (5) The operator F is annihilated by a separable¹⁹ polynomial $f \in \mathbb{k}[t]$ that is completely factorizable over \mathbb{k} as a product of linear factors.

Proof The equivalences (2) \iff (1) \iff (4) and the implication (1) \Rightarrow (3) are evident from the discussion preceding the proposition. The equivalence (4) \iff (5) follows at once from Corollary 15.3. If (3) holds, then $\sum_{\lambda \in \text{Spec } F} \dim V_\lambda = \deg \chi_F = \dim V$. Hence $\bigoplus_{\lambda \in \text{Spec}(F)} V_\lambda = V$. Thus, (3) \Rightarrow (1). \square

Corollary 15.9 *The restriction of a diagonalizable operator F to an F -invariant subspace is diagonalizable as well.*

Proof This is provided by (5). \square

Corollary 15.10 *Over an algebraically closed field, diagonalizability is equivalent to semisimplicity.*

Proof The monic irreducible polynomials over an algebraically closed field are exhausted by the linear binomials $t - \lambda$. \square

Exercise 15.16 Give an example of a nondiagonalizable semisimple linear operator over \mathbb{R} .

15.2.7 Annihilating Polynomials

If we know a polynomial $f \in \mathbb{k}[x]$ that annihilates an operator $F : V \rightarrow V$ and know the irreducible factorization of f in $\mathbb{k}[t]$ as well, then by Corollary 15.3, the collection of elementary divisors $\mathcal{E}\ell(F)$ becomes restricted to a finite number of effectively enumerable possibilities. Often, this allows us to decompose V into a direct sum of F -invariant subspaces defined in intrinsic terms of the F -action on V .

Example 15.2 (Involutions) Assume that $\text{char } \mathbb{k} \neq 2$. A linear operator $\sigma : V \rightarrow V$ is called an *involution* if $\sigma^2 = \text{Id}_V$. Thus, σ is annihilated by the polynomial $t^2 - 1 = (t + 1)(t - 1)$, which satisfies condition (5) of Proposition 15.6. We conclude that

¹⁹That is, without multiple roots.

either $\sigma = \pm \text{Id}_V$ or $V = V_+ \oplus V_-$, where

$$V_+ = \ker(\sigma - \text{Id}_V) = \text{im}(\sigma + \text{Id}_V) \quad \text{and} \quad V_- = \ker(\sigma + \text{Id}_V) = \text{im}(\sigma - \text{Id}_V)$$

are ± 1 -eigenspaces of σ . An arbitrary vector $v \in V$ is decomposed in terms of them as

$$v = v_+ + v_- = \frac{v + Fv}{2} + \frac{v - Fv}{2},$$

with $v_{\pm} = (v \pm Fv)/2 \in V_{\pm}$.

Example 15.3 (Projectors) A linear operator $\pi : V \rightarrow V$ is called a *projector*²⁰ if $\pi^2 = \pi$. Thus, π is annihilated by the polynomial $t^2 - t = t(t - 1)$, which also satisfies condition (5) of Proposition 15.6. We conclude that either $\pi = 0$, or $\pi = \text{Id}$, or $V = V_0 \oplus V_1$, where $V_0 = \ker \pi$ and $V_1 = \{v \in V \mid \pi v = v\}$ consists of the fixed vectors of π . The first two projectors are called *trivial*. The third projects V onto $\text{im } \pi$ along $\ker \pi$ (which explains the terminology). Note that for every idempotent π , the operator $\text{Id}_V - \pi$ is idempotent, too, and projects V onto $\ker \pi$ along $\text{im } \pi$. Thus, to produce a direct sum decomposition $V = U \oplus W$, it is necessary and sufficient to choose two idempotent operators $\pi_1 = \pi_1^2$, $\pi_2 = \pi_2^2$ on V such that $\pi_1 + \pi_2 = \text{Id}_V$ and $\pi_1\pi_2 = \pi_2\pi_1 = 0$.

Exercise 15.17 Deduce from these relations that $\ker \pi_1 = \text{im } \pi_2$ and $\text{im } \pi_1 = \ker \pi_2$.

Proposition 15.7 Assume that the operator $F : V \rightarrow V$ is annihilated by the polynomial $q \in \mathbb{k}[t]$ factored in $\mathbb{k}[t]$ as

$$q = q_1 \cdot q_2 \cdots q_r, \text{ where } \forall i, j \text{ GCD}(q_i, q_j) = 1.$$

Let $Q_i = \prod_{v \neq i} q_v = q/q_i$. Then $\ker q_i(F) = \text{im } Q_i(F)$ for each i , all these subspaces are F -invariant, and V is a direct sum of those of them that are nonzero.

Proof The invariance of $\ker q_i(F)$ is obvious: $q_i(F)v = 0 \Rightarrow q_i(F)Fv = Fq_i(F)v = 0$. The inclusion $\text{im } Q_i(F) \subset \ker q_i(F)$ follows from the vanishing of $q_i(F) \circ Q_i(F) = q(F) = 0$. Let us show that $\ker q_i(F) \cap \sum_{v \neq i} \ker q_v(F) = 0$, i.e., that the sum of the nonzero subspaces $\ker q_i(F)$ is a direct sum. Since all q_i are mutually coprime, $\text{GCD}(q_i, Q_i) = 1$ as well. Hence there exist $g, h \in \mathbb{k}[t]$ such that $1 = g(t)q_i(t) + h(t)Q_i(t)$. Substituting $t = F$, we get $\text{Id} = g(F) \circ q_i(F) + h(F) \circ Q_i(F)$. Applying both sides to any vector $v \in \ker q_i(F) \cap \sum_{j \neq i} \ker q_j$, we get $v = g(F) \circ q_i(F)v + h(F) \circ Q_i(F)v = 0$, because $\ker Q_i(F)$ contains all $\ker q_v(F)$ with $v \neq i$. Finally, let us show that the subspaces $\text{im } Q_i$ span

²⁰Or an *idempotent* operator.

V . Since $\text{GCD}(Q_1, Q_2, \dots, Q_r) = 1$, there exist $h_1, h_2, \dots, h_r \in \mathbb{k}[t]$ such that $1 = \sum Q_i(t) \cdot h_i(t)$. Substitute $t = F$ and apply both sides to any $v \in V$. We see that $v = \sum Q_i(F)h_i(F)v \subset \sum \text{im } Q_i(F)$. This forces $\text{im } Q_i(F) = \ker q_i(F)$ and $\bigoplus \ker q_i(F) = V$. \square

15.3 Jordan Decomposition

15.3.1 Jordan Normal Form

In this section, we assume by default that the ground field \mathbb{k} is algebraically closed. In this case, the monic irreducible elements of $\mathbb{k}[t]$ are exhausted by the linear binomials $(t - \lambda)$. Thus, by Theorem 15.1, every linear operator $F : V \rightarrow V$ is similar to multiplication by t in the direct sum of residue modules

$$\frac{\mathbb{k}[t]}{((t - \lambda_1)^{m_1})} \oplus \cdots \oplus \frac{\mathbb{k}[t]}{((t - \lambda_s)^{m_s})}, \quad (15.7)$$

and two such multiplication operators in the sums

$$\frac{\mathbb{k}[t]}{((t - \nu_1)^{n_1})} \oplus \cdots \oplus \frac{\mathbb{k}[t]}{((t - \nu_r)^{n_r})} \quad \text{and} \quad \frac{\mathbb{k}[t]}{((t - \mu_1)^{m_1})} \oplus \cdots \oplus \frac{\mathbb{k}[t]}{((t - \mu_s)^{m_s})}$$

are similar if and only if $r = s$, and after appropriate renumbering we get $\mu_i = \nu_i$, $m_i = n_i$ for all i . Multiplication by $t = \lambda + (t - \lambda)$ in $\mathbb{k}[t]/((t - \lambda)^m)$ is the sum of the homothety $\lambda E : f \mapsto \lambda f$ and nilpotent operator $\eta : f \mapsto (t - \lambda) \cdot f$, for which the classes of powers

$$(t - \lambda)^{m-1}, \quad (t - \lambda)^{m-2}, \dots, (t - \lambda), \quad 1 \quad (15.8)$$

form a Jordan chain²¹ of length m . In the basis (15.8), multiplication by t has the matrix

$$J_m(\lambda) \stackrel{\text{def}}{=} \lambda E + J_m(0) = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} \quad (15.9)$$

of size $m \times m$ with zeros in all other cells. It is called a *Jordan block* of size m with eigenvalue λ .

²¹See Sect. 15.2.1 on p. 367.

Corollary 15.11 (Jordan Normal Form) *Every linear operator $F : V \rightarrow V$ over an algebraically closed field \mathbb{k} has a basis in which F has a block-diagonal matrix*

$$\begin{pmatrix} J_{m_1}(\lambda_1) & & & \\ & J_{m_2}(\lambda_2) & & \\ & & \ddots & \\ & & & J_{m_k}(\lambda_k) \end{pmatrix} \quad (15.10)$$

formed by Jordan blocks $J_{m_1}(\lambda_1), J_{m_2}(\lambda_2), \dots, J_{m_k}(\lambda_k)$, where repeated blocks are allowed as well. Up to permutations of blocks, the matrix (15.10) does not depend on the choice of basis in question. Two operators are similar if and only if their matrices (15.10) coincide up to a permutation of blocks. \square

Definition 15.1 The matrix (15.10) is called the *Jordan normal form* of the operator F . Every basis of V in which the matrix of F takes its Jordan normal form is called a *Jordan basis* for F .

15.3.2 Root Decomposition

Let $F : V \rightarrow V$ be a linear operator over an algebraically closed field and let $\lambda \in \text{Spec}(F)$ be an eigenvalue of λ . The submodule of $(t - \lambda)$ -torsion in V_F is called the *root subspace* of F associated with $\lambda \in \text{Spec } F$, or just λ -*root* subspace for short. We denote it by

$$\begin{aligned} K_\lambda &= \{v \in V \mid \exists m \in \mathbb{N} : (\lambda \text{ Id} - F)^m v = 0\} \\ &= \bigcup_{m \geq 1} \ker(\lambda \text{ Id} - F)^m \\ &= \ker(\lambda \text{ Id} - F)^{m_\lambda}, \end{aligned} \quad (15.11)$$

where $m_\lambda = m_{(t-\lambda)}(F)$ is the index²² of $t - \lambda$ in $\mathcal{E}_\ell(F)$. Since $0 \neq V_\lambda \subset K_\lambda$ for all $\lambda \in \text{Spec}(F)$, all the root subspaces are nonzero. The canonical decomposition of V_F into a direct sum of $(t - \lambda)$ -torsion submodules looks like $V = \bigoplus_{\lambda \in \text{Spec } F} K_\lambda$ and is called the *root decomposition* of F .

Exercise 15.18 Prove the existence of the root decomposition by means of Proposition 15.7 and the Cayley–Hamilton identity without any reference to the general theory from Chap. 14.

The total number of Jordan blocks of size m with eigenvalue λ in the Jordan normal form of an operator F is equal to the number of length- m rows in the Young diagram

²²That is, the maximal integer m such that $(t - \lambda)^m \in \mathcal{E}_\ell(F)$ (see Sect. 15.1.5 on p. 365).

ν of the nilpotent operator

$$(\lambda \text{ Id} - F)|_{K_\lambda} : K_\lambda \rightarrow K_\lambda .$$

By formula (15.6) on p. 368, the k th column of this diagram has length

$$\nu_k' = \dim \ker(\lambda \text{ Id} - F)^k - \dim \ker(\lambda \text{ Id} - F)^{k-1} . \quad (15.12)$$

Therefore, the Jordan normal form of F can be calculated as follows. Perform the irreducible factorization of the characteristic polynomial:

$$\chi_F(t) = \prod_{\lambda \in \text{Spec}(F)} (x - \lambda)^{d_\lambda} .$$

Then for each $\lambda \in \text{Spec}(F)$ and each integer k in the range $1 \leq k \leq d_\lambda$, calculate

$$\dim \ker(\lambda \text{ Id} - F)^k = \dim V - \text{rk}(\lambda \text{ Id} - F)^k$$

while these numbers are strictly decreasing. Then draw the Young diagram ν whose columns have lengths (15.12). The number of blocks $J_\ell(\lambda)$ equals the number of length- ℓ rows in ν .

15.3.3 Commuting Operators

If linear operators $F, G : V \rightarrow V$ over an arbitrary field \mathbb{k} commute, then for every $f \in \mathbb{k}[t]$, the subspaces $\ker f(F)$ and $\text{im} f(F)$ are G -invariant, because

$$\begin{aligned} f(F)v = 0 &\Rightarrow f(F)Gv = Gf(F)v = 0 \\ v = f(F)w &\Rightarrow Gv = Gf(F)w = f(F)Gw . \end{aligned}$$

In particular, the eigenspaces $V_\lambda = \ker(F - \lambda E)$ and root spaces

$$K_\lambda = \ker(\lambda \text{ Id} - F)^{m_\lambda}$$

of the operator F are sent to themselves by every linear operator commuting with F .

Proposition 15.8 *Every set of commuting linear operators over an algebraically closed field has a common eigenvector. Over an arbitrary field, every set of diagonalizable commuting operators can be simultaneously diagonalized in a common basis.*

Proof By induction on $\dim V$, where V is the space on which the operators act. Both statements are obvious if all the operators are scalar dilations, which holds, in

particular, for $\dim V = 1$. Assume that one of the operators, call it F , is nonscalar. To prove the first statement, note that F has a proper eigenspace $0 \neq V_\lambda \subsetneq V$ sent to itself by all operators. By induction, all operators have a common eigenvector within V_λ . To prove the second statement, consider the decomposition of V in a direct sum of eigenspaces of F : $V = \bigoplus_{\lambda \in \text{Spec}(F)} V_\lambda$. All operators send each V_λ to itself and are diagonalizable on V_λ by Corollary 15.9 on p. 373. Thus, they can be simultaneously diagonalized on each V_λ . \square

15.3.4 Nilpotent and Diagonalizable Components

Theorem 15.3 (Jordan Decomposition) *For every linear operator F over an algebraically closed field \mathbb{k} , there exists a unique pair of operators F_s, F_n such that F_n is nilpotent, F_s is diagonalizable, $F = F_s + F_n$, and $F_s F_n = F_n F_s$. Moreover, $F_s = f_s(F)$ and $F_n = f_n(F)$ for appropriate polynomials $f_n, f_s \in \mathbb{k}[t]$ without constant terms. In particular, F_s and F_n commute with every operator commuting with F , and all F -invariant subspaces are invariant for both operators F_s, F_n as well.*

Proof Realize F as multiplication by t in a direct sum of residue modules

$$\frac{\mathbb{k}[t]}{((t - \lambda_1)^{m_1})} \oplus \cdots \oplus \frac{\mathbb{k}[t]}{((t - \lambda_s)^{m_s})}, \quad (15.13)$$

and let $\text{Spec } F = \{\lambda_1, \lambda_2, \dots, \lambda_r\}$. For each $i = 1, 2, \dots, r$, let us fix some integer $a_i > m_{\lambda_i}(F)$, where $m_{\lambda_i}(F)$ is the maximal integer m such that $(t - \lambda_i)^m \in \mathcal{E}\ell(F)$. By the Chinese remainder theorem, there exist $f_1, f_2, \dots, f_r \in \mathbb{k}[t]$ such that

$$f_v(t) \equiv \begin{cases} 1 \pmod{(t - \lambda_v)^{a_v}}, \\ 0 \pmod{(t - \lambda_\mu)^{a_\mu}} \text{ for } \mu \neq v. \end{cases}$$

If $\lambda_v \neq 0$, then the polynomial t is invertible modulo $(t - \lambda_v)^{a_v}$, i.e., there exists a polynomial $g_v(t)$ such that $t \cdot g_v(t) \equiv \lambda_v \pmod{(t - \lambda_v)^{a_v}}$. For $\lambda_v = 0$, we put $g_v = 0$. Therefore,

$$f_s(t) \stackrel{\text{def}}{=} t \sum_{v=1}^r g_v(t) f_v(t) \equiv \lambda_v \pmod{(t - \lambda_v)^{a_v}}$$

for each v . The polynomial $f_s(t)$ has zero constant term, and multiplication by $f_s(t)$ acts on each direct summand $\mathbb{k}[t]/((t - \lambda_v)^m)$ in the decomposition (15.13) as multiplication by λ_v . Thus, the operator $F_s \stackrel{\text{def}}{=} f_s(F)$ is diagonalizable. The operator $F_n \stackrel{\text{def}}{=} F - F_s$ acts on $\mathbb{k}[t]/((t - \lambda_v)^m)$ as multiplication by $t - \lambda_v$. Hence, F_n is nilpotent. As polynomials in F , both operators F_s, F_n commute with F and with

each other. This proves the existence of F_s, F_n as well as the last two statements. It remains to check uniqueness. Let $F = F'_s + F'_n$ be some other decomposition satisfying the first statement. Since F'_s and F'_n commute, they both commute with $F = F'_s + F'_n$ and with every polynomial of F including F_s and F_n . Therefore, each λ -eigenspace V_λ of F_s is F'_s -invariant, and the restriction $F'_s|_{V_\lambda}$ is diagonalizable. This forces $F'_s|_{V_\lambda} = \lambda \cdot \text{Id}_{V_\lambda} = F_s|_{V_\lambda}$, because the difference $F_s - F'_s = F'_n - F_n$ is nilpotent and therefore has zero spectrum.

Exercise 15.19 Check that the sum of two commuting nilpotent operators is also nilpotent.

We conclude that $F'_s = F_s$ and therefore $F'_n = F - F'_s = F - F_s = F_n$. \square

Definition 15.2 The operators F_s and F_n from Theorem 15.3 are called the *semisimple* and *nilpotent* components of the operator F .

15.4 Functions of Operators

15.4.1 Evaluation of Functions on an Operator

In this section we always assume that $\mathbb{K} = \mathbb{C}$. Let $F : V \rightarrow V$ be a linear operator with $\text{Spec } F = \{\lambda_1, \lambda_2, \dots, \lambda_r\}$. Recall that we write $m_\lambda = m_{(t-\lambda)}(F)$ for the maximal integer m such that $(t - \lambda)^m \in \mathcal{E}\ell(F)$ and write

$$\mu_F(t) = \prod_{\lambda \in \text{Spec } F} (t - \lambda)^{m_\lambda}$$

for the minimal polynomial of F . We say that a \mathbb{C} -subalgebra \mathcal{C} in the algebra $\mathbb{C}^{\mathbb{C}}$ of all functions $\mathbb{C} \rightarrow \mathbb{C}$ is *suitable* for evaluation at F if $\mathcal{C} \supset \mathbb{C}[t]$ and for each $\lambda \in \text{Spec } F$ and $f \in \mathcal{C}$, there exists $g \in \mathcal{C}$ such that

$$f(z) = f(\lambda) + \frac{f'(\lambda)}{1!}(z-\lambda) + \dots + \frac{f^{(m_\lambda-1)}(\lambda)}{(m_\lambda-1)!}(z-\lambda)^{m_\lambda-1} + g(z) \cdot (z-\lambda)^{m_\lambda}, \quad (15.14)$$

where $f^{(k)} = d^k f / dz^k$ means the k th derivative. For example, suitable for evaluation at F is the algebra of all functions $f : \mathbb{C} \rightarrow \mathbb{C}$ such that for each $\lambda \in \text{Spec } F$, the Taylor expansion of f at λ has nonzero radius of convergence. In particular, the algebra of all analytic functions²³ $\mathbb{C} \rightarrow \mathbb{C}$ is suitable for evaluation at any linear operator F . Our terminology is justified by the following claim.

²³That is, power series converging everywhere in \mathbb{C} .

Theorem 15.4 *Let a subalgebra $\mathcal{C} \subset \mathbb{C}^{\mathbb{C}}$ be suitable for evaluation at an operator $F : V \rightarrow V$. Then there exists a unique homomorphism of \mathbb{C} -algebras $\text{ev}_F : \mathcal{C} \rightarrow \text{End } V$ whose restriction to the polynomial subalgebra $\mathbb{C}[t] \subset \mathcal{C}$ coincides with the standard evaluation of polynomials $f(t) \mapsto f(F)$. Moreover, for every $f \in \mathcal{C}$, there exists a polynomial $P_{f,F} \in \mathbb{C}[t]$ such that $f(F) = P_{f,F}(F)$. The residue class of the polynomial $P_{f,F}$ modulo (μ_F) is uniquely determined by the equalities $P_{f,F}^{(k)}(\lambda) = f^{(k)}(\lambda)$ for all $0 \leq k \leq m_\lambda - 1$ and all $\lambda \in \text{Spec } F$, where $P_{f,F}^{(k)}$ means the k th derivative.*

Proof Let $\text{ev}_F : \mathcal{C} \rightarrow \mathbb{C}$ be a required homomorphism of \mathbb{C} -algebras. Fix an arbitrary function $f \in \mathcal{C}$ and evaluate both sides of (15.14) at F . This leads to the equality

$$f(F) = f(\lambda) \cdot E + f'(\lambda) \cdot (F - \lambda E) + \cdots + \frac{f^{(m_\lambda-1)}(\lambda)}{(m_\lambda-1)!} (F - \lambda E)^{m_\lambda-1} + g_\lambda(F) (F - \lambda E)^{m_\lambda}. \quad (15.15)$$

Since the last summand annihilates the λ -root subspace $K_\lambda = \ker(F - \lambda E)^{m_\lambda}$ of F , the operator $f(F)$ sends K_λ to itself and acts there as $f_\lambda(F)$, where

$$f_\lambda(t) = f(\lambda) + f'(\lambda) \cdot (t - \lambda) + \cdots + \frac{f^{(m_\lambda-1)}(\lambda)}{(m_\lambda-1)!} (t - \lambda)^{m_\lambda-1} \quad (15.16)$$

is the $(m_\lambda - 1)$ th jet of the function f at the point $\lambda \in \mathbb{C}$. By the Chinese remainder theorem, there exists a unique residue class $[P_{f,F}] \in \mathbb{C}[t] / (\mu_F)$ congruent to $f_\lambda(t)$ modulo $(t - \lambda)^{m_\lambda}$ for all $\lambda \in \text{Spec } F$. Therefore, $f(F)$ acts on each root subspace K_λ exactly as $P_{f,F}(F)$. Hence, $f(F) = P_{f,F}(F)$ on the whole space $V = \bigoplus_{\lambda \in \text{Spec } F} K_\lambda$. This establishes the uniqueness of evaluation and the last statement of the theorem. It remains to check that the rule $f(F) \stackrel{\text{def}}{=} P_{f,F}(F)$ actually defines a homomorphism of \mathbb{C} -algebras $\mathcal{C} \rightarrow \text{End } V$. Write $j_\lambda^m : \mathcal{C} \rightarrow \mathbb{C}[t] / ((t - \lambda)^m)$ for the map sending a function $f \in \mathcal{C}$ to its $(m - 1)$ th jet at λ ,

$$j_\lambda^m f \stackrel{\text{def}}{=} \sum_{k=0}^{m-1} \frac{1}{k!} f^{(k)}(\lambda) (t - \lambda)^k \bmod (t - \lambda)^m,$$

and consider the direct product of these maps over all points $\lambda \in \text{Spec } F$:

$$\begin{aligned} j : \mathcal{C} &\rightarrow \prod_{\lambda \in \text{Spec } F} \mathbb{C}[t] / ((t - \lambda)^{m_\lambda}) \simeq \mathbb{C}[t] / (\mu_F), \\ f &\mapsto (j_{\lambda_1}^{m_{\lambda_1}-1} f, \dots, j_{\lambda_r}^{m_{\lambda_r}-1} f). \end{aligned} \quad (15.17)$$

Exercise 15.20 Verify that (15.17) is a homomorphism of \mathbb{C} -algebras.

Our map $f \mapsto P_{f,F}(F)$ is the homomorphism (15.17) followed by the standard evaluation of polynomials $\text{ev}_F : \mathbb{C}[t]/(\mu_F) \rightarrow \text{End } V$. Therefore, it is a homomorphism of \mathbb{C} -algebras as well. \square

15.4.2 Interpolating Polynomial

A polynomial $P_{f,F} \in \mathbb{C}[z]$ from Theorem 15.4 is called an *interpolating polynomial* for the evaluation of a function $f \in \mathcal{C}$ at an operator $F : V \rightarrow V$. Note that it crucially depends on both the function and the operator. In particular, the values of the same function on different operators are usually evaluated by completely different interpolating polynomials. At the same time, an interpolating polynomial is defined only up to addition of polynomial multiples of the minimal polynomial μ_F . In practical computations, if the irreducible factorization of the characteristic polynomial is known,

$$\chi_F = \prod_{\lambda \in \text{Spec } F} (t - \lambda)^{N_\lambda},$$

then certainly $N_\lambda \geq m_\lambda$, and we can take $P_{f,F}$ to be equal to the unique polynomial of degree at most $\dim V$ such that $P_{f,F}^{(k)}(\lambda) = f^{(k)}(\lambda)$ for all $\lambda \in \text{Spec } F$ and $0 \leq k \leq N_\lambda - 1$.

Example 15.4 (Power Function and Linear Recurrence Equations) The solution of the linear recurrence equation

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \cdots + a_m z_{k-m} = 0 \quad (15.18)$$

of order m in the unknown sequence (z_n) is equivalent to evaluation of the power function $t \mapsto t^n$ on the *shifting matrix* of the sequence,

$$S = \begin{pmatrix} 0 & 0 & \cdots & 0 & \alpha_m \\ 1 & 0 & \ddots & 0 & \alpha_{m-1} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \alpha_2 \\ 0 & \cdots & 0 & 1 & \alpha_1 \end{pmatrix},$$

which has size $m \times m$ and is uniquely determined by

$$(z_{k+1}, z_{k+2}, \dots, z_{k+m}) \cdot S = (z_{k+2}, z_{k+3}, \dots, z_{k+m+1}).$$

Indeed, the n th term of the desired sequence is equal to the first coordinate of the vector

$$(z_n, z_{n+1}, \dots, z_{z+m-1}) = (z_0, z_1, \dots, z_{m-1}) \cdot S^n,$$

as soon the initial terms $(z_0, z_1, \dots, z_{m-1})$ are given. We know from Theorem 15.4 that S^n can be evaluated by substitution $t = S$ into the interpolating polynomial $P_{z^n, S}(t)$, whose degree is at most m , and the coefficients are found from a system of $m + 1$ usual linear equations. Note that as soon as S^n has been found, we can solve the same recurrence equation for different initial data almost without additional computations.

Example 15.5 (Fibonacci Numbers Revisited) The shifting matrix for the Fibonacci numbers²⁴ $z_n = z_{n-1} + z_{n-2}$ is $S = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Its characteristic polynomial $\chi_S(t) = t^2 - t \operatorname{tr} S + \det S = t^2 - t - 1 = (t - \lambda_+)(t - \lambda_-)$ has roots $\lambda_{\pm} = (1 \pm \sqrt{5})/2$, and the power function z^n takes values λ_{\pm}^n on them. The interpolating polynomial $P_{z^n, S}(t) = at + b$ is linear. Its coefficients are found at once by Cramer's rules from the equations

$$\begin{cases} a\lambda_+ + b = \lambda_+^n, \\ a\lambda_- + b = \lambda_-^n, \end{cases}$$

and they are equal to $a = (\lambda_+^n - \lambda_-^n) / (\lambda_+ - \lambda_-)$, $b = (\lambda_+^{n+1} - \lambda_-^{n+1}) / (\lambda_+ - \lambda_-)$. Therefore,

$$S^n = aS + bE = \begin{pmatrix} b & a \\ a & a+b \end{pmatrix}.$$

For the classical initial terms $z_0 = 0$, $z_1 = 1$, we get $(z_n, z_{n+1}) = (0, 1) \cdot S^n = (a, a + b)$, i.e.,

$$z_n = a = \frac{\left(\left(1 + \sqrt{5}\right)/2\right)^n - \left(\left(1 - \sqrt{5}\right)/2\right)^n}{\sqrt{5}}.$$

Proposition 15.9 *Under the conditions of Theorem 15.4, the spectrum $\operatorname{Spec} f(F)$ consists of the numbers $f(\lambda)$, $\lambda \in \operatorname{Spec} F$. If $f'(\lambda) \neq 0$, then the elementary divisors $(t - \lambda)^m \in \mathcal{E}\ell(F)$ are in bijection with the elementary divisors $(t - f(\lambda))^m \in \mathcal{E}\ell(f(F))$. If $f'(\lambda) = 0$, then each elementary divisor $t - \lambda \in \mathcal{E}\ell(F)$ produces an elementary divisor $t - f(\lambda) \in \mathcal{E}\ell(f(F))$, and each elementary divisor $(t - \lambda)^m \in \mathcal{E}\ell(F)$ with $m > 1$*

²⁴Compare with Example 4.4 on p. 81.

produces more than one elementary divisor $(t - f(\lambda))^\ell \in \mathcal{E}\ell(f(F))$ with $\ell < m$. The whole of $\mathcal{E}\ell(f(F))$ is exhausted by the elementary divisors just described.

Proof Realize F as multiplication by t in

$$V = \frac{\mathbb{C}[t]}{((t - \lambda_1)^{s_1})} \oplus \cdots \oplus \frac{\mathbb{C}[t]}{((t - \lambda_r)^{s_r})}.$$

The proof of Theorem 15.4 shows that the semisimple and nilpotent components of the operator $f(F)$ restricted to the $(t - \lambda)$ -torsion submodule K_λ are $f_s(F) = f(\lambda) \cdot \text{Id}$ and $f_n(F) = f'(\lambda) \cdot \eta + \frac{1}{2}f''(\lambda) \cdot \eta^2 + \cdots$, where η denotes the nilpotent operator provided by multiplication by $(t - \lambda)$. The operator η has exactly one Jordan chain of maximal length k on each direct summand $\mathbb{C}[t]/((t - \lambda)^k)$ within K_λ . If $f'(\lambda) \neq 0$, then $f_n^{k-1}(F) = f'(\lambda)^{k-1} \cdot \eta^{k-1} \neq 0$. This forces $f_n(F)$ to have exactly one Jordan chain of length k on $\mathbb{C}[t]/((t - \lambda)^k)$ as well. If $f'(\lambda) = 0$ and $m > 1$, we get $f_n^\ell(F) = 0$ for some $\ell < k$. Therefore, the cyclic type of $f_n(F)$ restricted to $\mathbb{C}[t]/((t - \lambda)^k)$ consists of more than one Jordan chain, which all are strictly shorter than k . \square

Exercise 15.21 Show that the matrix $J_m^{-1}(\lambda)$ inverse to the Jordan block²⁵ of size m is conjugate to the Jordan block $J_m(\lambda^{-1})$.

15.4.3 Comparison with Analytic Approaches

Analytic methods to extend the evaluation map

$$\text{ev}_F : \mathbb{C}[z] \rightarrow \text{Mat}_n(\mathbb{C}), \quad z \mapsto F \in \text{Mat}_n(\mathbb{C}),$$

to some larger algebra $\mathcal{C} \supset \mathbb{C}[z]$ of functions $\mathbb{C} \rightarrow \mathbb{C}$ usually provide both spaces \mathcal{C} , $\text{Mat}_n(\mathbb{C})$ with suitable topologies, then approximate functions $f \in \mathcal{C}$ by sequences of polynomials f_ν converging to f as $\nu \rightarrow \infty$, and then define $f(F)$ as a limit of matrices $f_\nu(F)$. Of course, one should check that $f(F)$ depends only on f but not on the choice of sequence approximating f and verify that the resulting map $\text{ev}_F : \mathcal{C} \rightarrow \text{Mat}_n(\mathbb{C})$ is a homomorphism of \mathbb{C} -algebras²⁶ (otherwise, it would probably be of no use). But whatever sequence of polynomials f_ν is used to approximate f , the corresponding sequence of matrices $f_\nu(F)$ lies in the linear span of powers F^m , $0 \leq m < n - 1$.

²⁵See formula (15.9) on p. 375.

²⁶It is highly edifying for students to realize this program independently using the standard topologies, in which the convergence of functions means the absolute convergence over every disk in \mathbb{C} , and the convergence of matrices means the convergence with respect to the distance on $\text{Mat}_n(\mathbb{C})$ defined by $|A, B| = \|A - B\|$, where $\|C\| \stackrel{\text{def}}{=} \max_{v \in \mathbb{C}^n \setminus 0} |Cv|/|v|$ and $|w|^2 \stackrel{\text{def}}{=} \sum |z_i|^2$ for $w = (z_1, z_2, \dots, z_n) \in \mathbb{C}^n$. A working test for such a realization could be a straightforward computation of $e^{J_n(\lambda)}$ directly from the definitions.

Thus, if the linear subspaces of $\text{Mat}_n(\mathbb{C})$ are closed in the topology used to define the evaluation, then $\lim_{f \rightarrow v} f(F)$ has to be a *polynomial* in F of degree at most $n - 1$. In other words, whatever analytic approach is used to construct the homomorphism $\text{ev}_F : \mathcal{C} \rightarrow \text{Mat}_n(\mathbb{C})$, its value on a given function $f \in \mathcal{C}$ should be computed a priori by Theorem 15.4.

Problems for Independent Solution to Chap. 15

Problem 15.1 Give an explicit example of a noncyclic²⁷ nonidentical linear operator.

Problem 15.2 Describe all invariant subspaces of an operator $F : \mathbb{K}^n \rightarrow \mathbb{K}^n$ whose matrix in the standard basis is diagonal with distinct diagonal elements.

Problem 15.3 Show that the minimal polynomial of every matrix of rank 1 over an arbitrary field is quadratic.

Problem 15.4 Is there some linear operator F over \mathbb{Q} such that (a) $\mu_F = t^3 - 1$ and $\chi_F = t^6 - 1$, (b) $\mu_F = (t - 1)(t - 2)$ and $\chi_F = (t - 1)^2(t - 2)^2$, (c) $\mu_F = (t - 1)^2(t - 2)^3$ and $\chi_F = (t - 1)^5(t - 2)^5$? If yes, give an explicit example, if not, explain why.

Problem 15.5 For $p = 2, 3, 5$, enumerate the conjugation classes of the matrices in (a) $\text{Mat}_2(\mathbb{F}_p)$, (b) $\text{GL}_2(\mathbb{F}_p)$, (c) $\text{SL}_2(\mathbb{F}_p)$.

Problem 15.6 Let the characteristic polynomial of an operator $F : V \rightarrow V$ be irreducible. Show that for every $v \in V \setminus 0$, the vectors $v, Fv, \dots, F^{\dim V - 1}v$ form a basis in V .

Problem 15.7 Let the degree of the minimal polynomial of an operator $F : V \rightarrow V$ be equal to $\dim V$. Show that every operator commuting with F can be written as a polynomial in F .

Problem 15.8 Given an operator F over an algebraically closed field \mathbb{K} , let the operator G commute with all operators commuting with F . Is it true that $G = f(F)$ for some $f \in \mathbb{K}[t]$?

Problem 15.9 Is there in $\text{Mat}_n(\mathbb{C})$ some $(n + 1)$ -dimensional subspace consisting of mutually commuting matrices?

Problem 15.10 For commuting operators F, G , prove that $(F + G)_s = F_s + G_s$ and $(F + G)_n = F_n + G_n$, where C_s, C_n mean the semisimple and nilpotent components²⁸ of the operator C .

Problem 15.11 Let the matrix of an operator $\mathbb{R}^n \rightarrow \mathbb{R}^n$ have $\lambda_1, \lambda_2, \dots, \lambda_n$ on the secondary diagonal and zeros everywhere else. For which $\lambda_1, \lambda_2, \dots, \lambda_n$ is this operator diagonalizable over \mathbb{R} ?

²⁷See Sect. 15.2.3 on p. 370.

²⁸See Definition 15.2 on p. 379.

Problem 15.12 Let a \mathbb{Q} -linear operator F satisfy the equality $F^3 = 6F^2 - 11F + 6E$. Can F be nondiagonalizable over \mathbb{Q} ?

Problem 15.13 Give an explicit example of two diagonalizable operators with nondiagonalizable composition.

Problem 15.14 Let the minimal polynomial of an operator $F : V \rightarrow V$ be factored as $\mu_F = g_1 g_2$, where $\text{GCD}(g_1, g_2) = 1$. Show that $V = U_1 \oplus U_2$, where both subspaces are F -invariant and the minimal polynomial of the restriction $F|_{U_i}$ equals g_i for both $i = 1, 2$.

Problem 15.15 Let an operator $F : \mathbb{K}^n \rightarrow \mathbb{K}^n$ have $\text{tr } F^k = 0$ for all $1 \leq k \leq n$. Show that F is nilpotent.

Problem 15.16 Let operators A, B satisfy the equality $AB - BA = B$. Show that B is nilpotent.

Problem 15.17* (Bart's Lemma) Show that for every $A, B \in \text{Mat}_n(\mathbb{C})$ such that $\text{rk}[A, B] = 1$, there exists a nonzero $v \in \mathbb{C}^n$ such that $Av = \lambda v$ and $Bv = \mu v$ for some $\lambda, \mu \in \mathbb{C}$.

Problem 15.18 Establish a bijection between the direct sum decompositions $V = U_1 \oplus U_2 \oplus \cdots \oplus U_s$ and collections of nontrivial projectors $\pi_1, \pi_2, \dots, \pi_s \in \text{End } V$ such that $\pi_1 + \pi_2 + \cdots + \pi_s = 1$ and $\pi_i \pi_j = \pi_j \pi_i = 0$ for all $i \neq j$.

Problem 15.19 Find the Jordan normal form of the square $J_m^2(\lambda)$ of the Jordan block $J_m(\lambda)$ (a) for $\lambda \neq 0$, (b) for $\lambda = 0$.

Problem 15.20 Write finite explicit expressions for the matrix elements of $f(J_m(\lambda))$ in terms of f and its derivatives at λ for every function $f : \mathbb{C} \rightarrow \mathbb{C}$ analytic in some neighborhood of $\lambda \in \mathbb{C}$.

Problem 15.21 Describe the eigenspaces and root subspaces of the following linear operators:

- (a) d/dx acting on the \mathbb{R} -linear span of functions $\sin(x), \cos(x), \dots, \sin(nx), \cos(nx)$;
- (b) d/dz acting on the functions $\mathbb{C} \rightarrow \mathbb{C}$ of the form $e^{\lambda z} f(z)$, where $f \in \mathbb{C}[z]_{\leq n}$ and $\lambda \in \mathbb{C}$ is fixed;
- (c) $x d/dx$ acting on $\mathbb{Q}[x]_{\leq n}$ and $\sum x_i \partial/\partial x_i$ acting on $\mathbb{Q}[x_1, x_2, \dots, x_n]_{\leq n}$;
- (d) $f(x) \mapsto f(x-1, y+1)$ acting on the \mathbb{Q} -linear span of the monomials $x^n y^m$ with $0 \leq m, n \leq 2$;
- (e) $f(x) \mapsto \int_0^1 (x^2 y + xy^2) f(y) dy$ acting on $\mathbb{R}[x]_{\leq 3}$;
- (f) $f(x) \mapsto f(ax+b)$, where $a, b \in \mathbb{Q}$ are fixed, acting on $\mathbb{Q}[x]_{\leq n}$.

Problem 15.22 Solve in $\text{Mat}_2(\mathbb{C})$ the equations

$$(a) X^2 = \begin{pmatrix} 3 & 1 \\ -1 & 5 \end{pmatrix}, \quad (b) X^2 = \begin{pmatrix} 6 & 2 \\ 3 & 7 \end{pmatrix}.$$

Problem 15.23 Compute A^{50} , $\sin A$, and e^A for the following matrices A :

(a) $\begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}$, (b) $\begin{pmatrix} 7 & -4 \\ 4 & -8 \end{pmatrix}$, (c) $\begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$, (d) $\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$.

Problem 15.24 Two operators $\mathbb{Q}^3 \rightarrow \mathbb{Q}^3$ have in the standard basis of \mathbb{Q}^3 the matrices

$$\begin{pmatrix} 5 & -1 & -1 \\ -1 & 5 & -1 \\ -1 & -1 & 5 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -6 & 2 & 3 \\ 2 & -3 & 6 \\ 3 & 6 & 2 \end{pmatrix}.$$

Find all subspaces in \mathbb{Q}^3 invariant simultaneously for the both operators.

Problem 15.25 Find the minimal polynomial over \mathbb{R} and over \mathbb{C} for the matrix

$$\begin{pmatrix} 5 & 5 & 1 & -10 \\ 2 & 5 & -2 & -9 \\ 0 & -1 & 1 & 0 \\ 3 & 4 & 0 & -8 \end{pmatrix}$$

and write the Jordan normal form of this matrix over \mathbb{C} .

Problem 15.26 Find the Jordan normal forms over the field \mathbb{C} for the following matrices:

(a) $\begin{pmatrix} 2 & 1 & -2 & 7 \\ 0 & 4 & -4 & 5 \\ 2 & 3 & -6 & 7 \\ 1 & 1 & -3 & 2 \end{pmatrix}$, (b) $\begin{pmatrix} 3 & 1 & -3 & 9 \\ 2 & 4 & -6 & 9 \\ 3 & 3 & -7 & 9 \\ 1 & 1 & -3 & 2 \end{pmatrix}$, (c) $\begin{pmatrix} -2 & -8 & 1 & -6 \\ 6 & 11 & -6 & 0 \\ 8 & 10 & -9 & -6 \\ -7 & -11 & 7 & 2 \end{pmatrix}$,

(d) $\begin{pmatrix} n & n-1 & n-2 & \cdots & 1 \\ 0 & n & n-1 & \cdots & 2 \\ 0 & 0 & n & \cdots & 3 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & n \end{pmatrix}$, (e) $\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$

Chapter 16

Bilinear Forms

In this section we assume by default that $\text{char } \mathbb{k} \neq 2$.

16.1 Bilinear Forms and Correlations

16.1.1 Space with Bilinear Form

Let V be a finite-dimensional vector space over a field \mathbb{k} . We write V^* for its dual space and $\langle *, * \rangle : V \times V^* \rightarrow \mathbb{k}$ for the pairing between vectors and covectors.¹ Recall that a map $\beta : V \times V \rightarrow \mathbb{k}$ is called a *bilinear form* on V if for all $\lambda \in \mathbb{k}$, $u, w \in V$, we have

$$\begin{aligned}\beta(u, \lambda w) &= \lambda \beta(u, w) = \beta(\lambda u, w), \\ \beta(u_1 + u_2, w_1 + w_2) &= \beta(u_1, w_1) + \beta(u_1, w_2) + \beta(u_2, w_1) + \beta(u_2, w_2).\end{aligned}$$

An example of a bilinear map is provided by the Euclidean structure on a real vector space.²

Exercise 16.1 Check that the bilinear maps form a vector subspace in the vector space of all functions $V \times V \rightarrow \mathbb{k}$.

Associated with a bilinear form $\beta : V \times V \rightarrow \mathbb{k}$ is the *right correlation map*

$$\beta : V \rightarrow V^*, \quad v \mapsto \beta(*, v), \quad (16.1)$$

¹See Example 7.6 on p. 161.

²See Sect. 10.1 on p. 229.

which sends a vector $v \in V$ to the covector $u \mapsto \beta(u, v)$. Every linear map (16.1) is a correlation map for a unique bilinear form on V , which is defined by

$$\beta(u, w) = \langle u, \beta w \rangle. \quad (16.2)$$

Exercise 16.2 Verify that the correspondence (16.2) establishes a linear isomorphism between the vector space of bilinear forms on V and the vector space $\text{Hom}(V, V^*)$ of linear maps $V \rightarrow V^*$.

We have deliberately denoted both the bilinear form and its right correlation by the same letter. In what follows, we will often make no distinction between them and will identify the space of bilinear forms with $\text{Hom}(V, V^*)$. Note that both have dimension n^2 as soon as $\dim V = n$. We call a pair (V, β) a *space with bilinear form* or just a *bilinear form* over \mathbb{k} . For two such spaces V_1, V_2 with bilinear forms β_1, β_2 , a linear map $f : V_1 \rightarrow V_2$ is called *isometric* or a *homomorphism* of bilinear forms if $\beta_1(v, w) = \beta_2(f(v), f(w))$ for all $v, w \in V_1$. In the language of right correlations, this means that the following diagram is commutative:

$$\begin{array}{ccc} V_1^* & \xleftarrow{f^*} & V_2^* \\ \beta_1 \uparrow & & \uparrow \beta_2 \\ V_1 & \xrightarrow{f} & V_2 \end{array} \quad (16.3)$$

i.e., $\beta_1 = f^* \beta_2 f$, where $f^* : V_2^* \rightarrow V_1^*$ is the dual linear map³ to f defined by $\langle v, f^* \xi \rangle = \langle f v, \xi \rangle$ for all $\xi \in V_2^*, v \in V$.

Exercise 16.3 Convince yourself that the relation $\beta_1(u, w) = \beta_2(f(u), f(w))$ for all $u, w \in V_1$ is equivalent to the commutativity of diagram (16.3).

Two bilinear forms β_1, β_2 on spaces V_1, V_2 are called *isomorphic* or *equivalent* if there exists an isometric linear isomorphism of vector spaces $V_1 \simeq V_2$.

16.1.2 Gramians

Let the vectors $e = (e_1, e_2, \dots, e_n)$ be a basis of V . Then every bilinear form β on V is uniquely determined by its values $b_{ij} = \beta(e_i, e_j)$ on the pairs of basis vectors. Indeed, given these values, then for every pair of vectors $u = \sum x_i e_i, w = \sum y_j e_j$, we have

$$\beta(u, w) = \beta\left(\sum_i x_i e_i, \sum_j y_j e_j\right) = \sum_{ij} b_{ij} x_i y_j. \quad (16.4)$$

³See Sect. 7.3 on p. 164.

The square matrix $B_e = (b_{ij})$ is called the *Gram matrix* of β in the basis e or simply the *Gramian*.

Exercise 16.4 Check that the matrix of right correlation $\beta : V \rightarrow V^*$ written in the dual bases e and e^* of V and V^* coincides with the Gram matrix B_e of the bilinear form $\beta : V \times V \rightarrow \mathbb{K}$ in the basis e .

If we write the basis vectors in the row matrix $e = (e_1, e_2, \dots, e_n)$ with elements in V and for $u, w \in V$ put $uw \stackrel{\text{def}}{=} \beta(u, w) \in \mathbb{K}$ as in Sect. 10.2 on p. 233, then $B_e = e^t e$, and the computation (16.4) for the vectors $u = ex$, $w = ey$, where $x, y \in \mathbb{K}^n$ are coordinate columns, can be rewritten as

$$uw = u^t w = x^t e^t ey = x^t B_e y. \quad (16.4')$$

More generally, associated with any two collections of vectors

$$u = (u_1, u_2, \dots, u_k), \quad w = (w_1, w_2, \dots, w_m),$$

is their reciprocal Gramian $B_{uw} = (\beta(u_i, w_j)) = u^t w$. The same computation as in Sect. 10.2 on p. 233 shows that for $u = eC_{eu}$ and $w = fC_{fw}$, we have

$$B_{uw} = u^t w = (eC_{eu})^t (fC_{fw}) = C_{eu}^t e^t f C_{fw} = C_{eu}^t B_{ef} C_{fw}. \quad (16.5)$$

In particular, for any two bases e, f in V related by $f = eC_{ef}$, we have

$$B_f = C_{ef}^t B_e C_{ef}. \quad (16.6)$$

It is instructive to compare this formula with the diagram (16.3).

16.1.3 Left Correlation

For a right correlation $\beta : V \rightarrow V^*$, its dual map $\beta^* : V^{**} \rightarrow V^*$ can be also viewed as a correlation $\beta^* : V \rightarrow V^*$ by means of the canonical identification⁴ $V^{**} \simeq V$. Correlations β and β^* are related by the equality $\langle u, \beta^* w \rangle = \langle w, \beta u \rangle$ for all $u, w \in V$. The correlation β^* is a right correlation for the bilinear form $\beta^*(u, w) = \langle u, \beta^* w \rangle = \langle w, \beta u \rangle = \beta(w, u)$ constructed from β by swapping the arguments. In the language of bilinear forms, the correlation $\beta^* : V \rightarrow V^*$ sends a vector $v \in V$ to the covector $w \mapsto \beta(v, w)$, i.e., maps $v \mapsto \beta(v, *)$. For this reason, β^* is called the *left correlation map* of the bilinear form β .

⁴See Sect. 7.1.2 on p. 158.

Exercise 16.5 Check that the matrix of the left correlation $\beta^* : V \rightarrow V^*$ in the dual bases \mathbf{e}, \mathbf{e}^* of V and V^* equals $B_{\mathbf{e}}^t$.

16.1.4 Nondegeneracy

A bilinear form β is called *nondegenerate*⁵ if it satisfies the equivalent conditions listed in Proposition 16.1 below. Otherwise, β is called *singular*.⁶

Proposition 16.1 (Nondegeneracy Criteria) *Let a bilinear form $\beta : V \times V \rightarrow \mathbb{K}$ have Gramian $B_{\mathbf{e}}$ in some basis $\mathbf{e} = (e_1, e_2, \dots, e_n)$ of V . The following conditions on β are equivalent:*

- (1) $\det B_{\mathbf{e}} \neq 0$.
- (2) $\forall w \in V \setminus 0 \exists u \in V : \beta(u, w) \neq 0$.
- (3) *The left correlation map $\beta^* : V \rightarrow V^*$ is an isomorphism.*
- (4) $\forall \xi \in V^*, \exists u_{\xi} \in V : \xi(v) = \beta(u_{\xi}, v)$ for all $v \in V$.
- (5) $\forall u \in V \setminus 0, \exists w \in V : \beta(u, w) \neq 0$.
- (6) *The right correlation map $\beta : V \rightarrow V^*$ is an isomorphism.*
- (7) $\forall \xi \in V^*, \exists w_{\xi} \in V : \xi(v) = \beta(v, w_{\xi})$ for all $v \in V$.

If these conditions hold, then condition (1) is valid for every basis of V , and both vectors u_{ξ}, w_{ξ} in (4), (7) are uniquely determined by the covector ξ .

Proof Conditions (2) and (4) mean that $\ker \beta^* = 0$ and $\operatorname{im} \beta^* = V^*$ respectively. Each of them is equivalent to (3), because $\dim V = \dim V^*$. For the same reason, conditions (5), (6), (7) are mutually equivalent as well. Since the operators β, β^* have transposed matrices $B_{\mathbf{e}}, B_{\mathbf{e}}^t$ in the dual bases \mathbf{e} and \mathbf{e}^* , the bijectivity of any one of them means that $\det B_{\mathbf{e}}^t = \det B_{\mathbf{e}} \neq 0$. \square

16.1.5 Kernels

If a bilinear form β is singular, then both subspaces

$$V^{\perp} = \ker \beta = \{u \in V \mid \forall v \in V \beta(v, u) = 0\}, \quad (16.7)$$

$$V^{\perp} = \ker \beta^* = \{u \in V \mid \forall v \in V \beta(u, v) = 0\}, \quad (16.8)$$

⁵Or *nonsingular*.

⁶Or *degenerate*.

are nonzero. They are called the *right* and *left kernels* of the bilinear form β . In general, $V^\perp \neq V^\perp$. Nevertheless, $\dim V^\perp = \dim V^\perp$, because β and β^* are dual to each other and therefore have equal ranks.⁷

Definition 16.1 The nonnegative integer $\text{rk } \beta \stackrel{\text{def}}{=} \dim \text{im } \beta = \dim \text{im } \beta^* = \text{codim } \ker \beta = \text{codim } \ker \beta^* = \text{rk } B$, where B is the Gramian of β in an arbitrary basis, is called the *rank* of the bilinear form β .

16.1.6 Nonsymmetric and (Skew)-Symmetric Forms

A dualization $\beta \mapsto \beta^*$ is a nontrivial linear involution⁸ on the space $\text{Hom}(V, V^*)$ of correlations. Therefore, the space of correlations splits into a direct sum of ± 1 -eigenspaces of the involution $*$:

$$\text{Hom}(V, V^*) = \text{Hom}_+(V, V^*) \oplus \text{Hom}_-(V, V^*),$$

where $\text{Hom}_+(V, V^*)$ consists of *symmetric* correlations $\beta = \beta^*$, whereas $\text{Hom}_-(V, V^*)$ is formed by *skew-symmetric* correlations $\beta = -\beta^*$. Such (skew)symmetric correlations produce *symmetric* and *skew-symmetric* bilinear forms, which satisfy for all $u, w \in V$ the identities $\beta(u, w) = \beta(w, u)$ and $\beta(u, w) = -\beta(w, u)$ respectively.

Exercise 16.6 Find $\dim \text{Hom}_\pm(V, V^*)$ for n -dimensional V .

All other bilinear forms $\beta(u, w) \neq \pm \beta(w, u)$ are called *nonsymmetric*. Associated with such a form β is the 2-dimensional subspace in $\text{Hom}(V, V^*)$ spanned by β and β^* . We call it the *pencil of correlations* of the bilinear form β and denote it by

$$\Pi_\beta = \{t_1\beta^* - t_0\beta : V \rightarrow V^* \mid t_0, t_1 \in \mathbb{k}\} \subset \text{Hom}(V, V^*). \quad (16.9)$$

These correlations produce bilinear forms $\beta_{(t_0, t_1)}(u, w) = t_1\beta(u, w) - t_0\beta(w, u)$. For $\text{char } \mathbb{k} \neq 2$, among these forms there exists a unique, up to proportionality, symmetric form $\beta_+ = (\beta + \beta^*)/2$ and skew-symmetric form $\beta_- = (\beta - \beta^*)/2$. Note that $\beta = \beta_+ + \beta_-$, and this equality is the unique decomposition of β as a sum of symmetric and skew-symmetric forms. The forms β_\pm are called the *symmetric* and *skew-symmetric components* of β .

Exercise 16.7 Give an example of a nondegenerate bilinear form β whose symmetric and skew-symmetric parts β_\pm are both singular.

⁷In dual bases, the matrices B'_e, B_e of these operators are transposes of each other and therefore have equal ranks by Theorem 7.3 on p. 166.

⁸See Example 15.2 on p. 373.

16.1.7 Characteristic Polynomial and Characteristic Values

The determinant

$$\chi_\beta(t_0, t_1) \stackrel{\text{def}}{=} \det(t_1 B_e - t_0 B_e^t) \in \mathbb{k}[t_0, t_1]$$

is called the *characteristic polynomial* of the bilinear form β . It is either homogeneous of degree $\dim V$ or vanishes identically. The transposition of variables $t_0 \leftrightarrow t_1$ multiplies χ_β by $(-1)^{\dim V}$:

$$\chi_\beta(t_0, t_1) = \det(t_1 B_e - t_0 B_e^t) = \det(t_1 B_e - t_0 B_e^t)^t \quad (16.10)$$

$$= \det(t_1 B_e^t - t_0 B_e) = (-1)^{\dim V} \chi_\beta(t_1, t_0). \quad (16.11)$$

Up to multiplication by a nonzero constant, χ_β does not depend on the choice of basis e whose Gramian B_e is used to evaluate the determinant, because in another basis $\varepsilon = e C_{e\varepsilon}$,

$$\det(t_1 B_\varepsilon - t_0 B_\varepsilon^t) = \det(t_1 C_{e\varepsilon}^t B_e C_{e\varepsilon} - t_0 C_{e\varepsilon}^t B_e^t C_{e\varepsilon}) \quad (16.12)$$

$$= \det(C_{e\varepsilon}^t) \det(t_1 B_e - t_0 B_e^t) \det(C_{e\varepsilon}) = \det(t_1 B_e - t_0 B_e^t) \cdot \det^2 C_{e\varepsilon}.$$

A bilinear form β is called *regular* if $\chi_\beta(t_0, t_1)$ is a nonzero polynomial. In this case, the roots of the characteristic polynomial on the projective line $\mathbb{P}_1 = \mathbb{P}(\Pi_\beta)$ are called the *characteristic values* of β . We write them as $\lambda = t_0/t_1 \in \mathbb{k} \sqcup \infty$, where $0 = 0 : 1$ and $\infty = 1 : 0$ may appear as well if the regular form is degenerate. The formula (16.10) forces the characteristic values different from ± 1 to split into the inverse pairs λ, λ^{-1} of equal multiplicities.

It follows from (16.12) that the characteristic values do not depend on the choice of basis. The computation (16.12) also shows that isomorphic bilinear forms have the same characteristic values. The characteristic values of the homogeneous coordinate $t = (t_0 : t_1)$ correspond to the degenerate correlations $\beta_t = t_1 \beta - t_0 \beta^* \in \Pi_\beta$ in the pencil (16.9). Every regular form β has at most $\dim V$ characteristic values (considered up to proportionality and counted with multiplicities). All the other correlations in the pencil Π_β are nonsingular.

The characteristic polynomial of a (skew) symmetric bilinear form β ,

$$\det(t_1 B_e - t_0 B_e^t) = \det(t_1 B_e \mp t_0 B_e) = (t_1 \mp t_0)^{\dim V} \det B_e,$$

is nonzero if and only if β is nondegenerate. Thus, the regularity of a (skew)symmetric bilinear form is equivalent to nonsingularity. Each nonsingular (skew)symmetric form has exactly one characteristic value. It has maximal multiplicity $\dim V$ and is equal to $(1 : 1)$ in the symmetric case and to $(1 : -1)$ in the skew-symmetric case. The degenerate form that corresponds to this value is the zero form.

Example 16.1 (Euclidean Form) The symmetric bilinear form on the coordinate space \mathbb{k}^n with unit Gramian E in the standard basis is called the *Euclidean form*. For $\mathbb{k} = \mathbb{R}$, it provides \mathbb{R}^n with a Euclidean structure. For other ground fields, the properties of the Euclidean form may be far from those usual in Euclidean geometry. For example, over \mathbb{C} , the nonzero vector $e_1 - ie_2 \in \mathbb{C}^2$ has zero inner product with itself. However, the Euclidean form is nonsingular. The bases in which the Gramian of the Euclidean form equals E are called *orthonormal*. The existence of an orthonormal basis for some bilinear form β means that β is equivalent to the Euclidean form. In Corollary 16.4 on p. 410 below we will see that every symmetric nonsingular bilinear form over an algebraically closed field \mathbb{k} of characteristic $\text{char } \mathbb{k} \neq 2$ is isomorphic to the Euclidean form.

Exercise 16.8 Find an n -dimensional subspace $U \subset \mathbb{C}^{2n}$ such that the Euclidean form on \mathbb{C}^n is restricted to the zero form on U .

Example 16.2 (hyperbolic Form) A symmetric bilinear form on an even-dimensional coordinate space \mathbb{k}^{2n} with Gramian

$$H = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix} \quad (16.13)$$

in the standard basis is called a *hyperbolic form*. Here E and 0 mean the identity and the zero $n \times n$ matrices. Therefore, $\det H = (-1)^n$ and H is nondegenerate. Over an algebraically closed field, the hyperbolic form is equivalent to the Euclidean form and admits an orthonormal basis formed by the vectors

$$\varepsilon_{2\nu-1} = (e_\nu - e_{n+\nu}) / \sqrt{-2} \quad \text{and} \quad \varepsilon_{2\nu} = (e_\nu + e_{n+\nu}) / \sqrt{2}, \quad 1 \leq \nu \leq n.$$

Over \mathbb{R} and \mathbb{Q} , the hyperbolic form is not equivalent to the Euclidean form, because for the latter form, the inner product of each nonzero vector with itself is positive, whereas the hyperbolic form vanishes identically on the linear span of the first n standard basis vectors. Every basis of \mathbb{k}^{2n} with Gramian (16.13) is called a *hyperbolic basis*.

Example 16.3 (Symplectic Form) A skew-symmetric form on an even-dimensional coordinate space \mathbb{k}^{2n} with Gramian

$$J = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \quad (16.14)$$

in the standard basis is called *symplectic*. A matrix J in (16.14) is called a *symplectic unit*. It has $J^2 = -E$ and $\det J = 1$. Thus, a symplectic form is nondegenerate. Every basis of \mathbb{k}^{2n} with Gramian (16.13) is called a *symplectic basis*. In Theorem 16.5 on p. 410 below, we will see that every nondegenerate skew-symmetric bilinear form

over any field is isomorphic to a symplectic form. In particular, this means that every space with a nonsingular skew-symmetric form must be even-dimensional.

Exercise 16.9 Check that every skew-symmetric square matrix of odd size is degenerate.

Example 16.4 (Euler Form) Write $D = d/dt : \mathbb{k}[t] \rightarrow \mathbb{k}[t]$ for the differentiation operator and $V = \mathbb{k}[D]/(D^{n+1})$ for the quotient ring of the ring $\mathbb{k}[D]$ of linear differential operators with constant coefficients⁹ by its principal ideal spanned by D^{n+1} . There is a *reverse of direction* involution on V defined by

$$\Phi(D) \mapsto \Phi^*(D) \stackrel{\text{def}}{=} \Phi(-D).$$

It takes the *shift operator* $T = e^D : f(t) \mapsto f(t+1)$ to the inverse shift operator $T^* = e^{-D} = T^{-1} : f(t) \mapsto f(t-1)$. Let us identify the space V^* dual to V with the space $\mathbb{k}[t]_{\leq n}$ of polynomials in t of degree at most n ,¹⁰ by means of the perfect pairing¹¹

$$\frac{\mathbb{k}[D]}{(D^{n+1})} \times \mathbb{k}[t]_{\leq n} \rightarrow \mathbb{k}, \quad \langle \Phi, f \rangle = \Phi^*f(0) = \text{ev}_0(\Phi(-D)f), \quad (16.15)$$

which contracts the residue class $\Phi(D) \pmod{D^{n+1}}$ and polynomial $f(t) \in \mathbb{k}[t]_{\leq n}$ to the constant term of the polynomial Φ^*f .

Exercise 16.10 Verify that the pairing (16.15) is well defined and perfect.¹² Find the basis of V dual to the standard monomial basis $1, t, \dots, t^n$ in V^* .

Put $\gamma_n(t) \stackrel{\text{def}}{=} \binom{t+n}{n} = (t+1)(t+2)\cdots(t+n)/n! \in V^*$ and define the correlation $h : V \rightarrow V^*$ by $h : \Phi \mapsto \Phi\gamma_n$. The bilinear form $h(\Phi, \Psi) \stackrel{\text{def}}{=} \Phi^*\Psi\gamma_n(0)$ corresponding to this correlation is called an *Euler form*.¹³ In the basis formed by the iterated shift operators $1, T, T^2, \dots, T^n$, the Euler form has an upper unitriangular

⁹This ring is isomorphic to the ring of polynomials $\mathbb{k}[x]$. It consists of differential operators $\Phi(D) = a_0D^n + a_1D^{n-1} + \cdots + a_{n-1}D + a_n$, which act on functions of t , e.g., on linear spaces $\mathbb{k}[t]$ and $\mathbb{k}[[t]]$ as in Sect. 4.4 on p. 88. Note that V models the “solution space” of the differential equation $d^n y/dt^n = 0$ in the unknown function $y = y(t)$.

¹⁰That is, with the actual solution space of the differential equation $d^n y/dt^n = 0$.

¹¹Note that it differs from that used in Problem 7.2 on p. 167 by changing the sign of D .

¹²See Sect. 7.1.4 on p. 160.

¹³It plays an important role in the theory of algebraic vector bundles on \mathbb{P}_n . In this theory, the roles of the vector spaces V and V^* are respectively played by the \mathbb{Z} -module of *difference operators* $\mathbb{Z}[\nabla]/(\nabla^{n+1})$, where $\nabla = 1 - e^D$, and by the \mathbb{Z} -module of *integer-valued polynomials*: $M_n = \{f \in \mathbb{Q}[t]_{\leq n} \mid f(\mathbb{Z}) \subset \mathbb{Z}\}$ (compare with Problem 14.30 on p. 359). Elements of the first module are the *characteristic classes* of vector bundles, whereas the elements of the second are the *Hilbert polynomials* of vector bundles. The formula computing the Euler form in terms of characteristic classes is known as the *Riemann–Roch theorem*.

Gramian with elements

$$h(T^i, T^j) = T^{j-i} \gamma_n(0) = \begin{cases} 0 & \text{for } j < i, \\ \binom{n+j-i}{n} & \text{for } j \geq i. \end{cases} \quad (16.16)$$

Every basis in which the Gramian of a nonsymmetric bilinear form β becomes upper unitriangular is called an *exceptional*¹⁴ (or *semiorthonormal*) basis for β .

16.2 Nondegenerate Forms

16.2.1 Dual Bases

In this section we consider a vector space V equipped with a *nondegenerate* bilinear form β . Let $\mathbf{e} = (e_1, e_2, \dots, e_n)$ be any basis of V . The preimages of the dual basis $\mathbf{e}^* = (e_1^*, e_2^*, \dots, e_n^*)$ in V^* under the left and right correlation maps $\beta^*, \beta : V \rightarrow V^*$ are respectively denoted by ${}^\vee \mathbf{e} = ({}^\vee e_1, {}^\vee e_2, \dots, {}^\vee e_n)$ and $\mathbf{e}^\vee = (e_1^\vee, e_2^\vee, \dots, e_n^\vee)$ and called the *left* and *right bases on V dual to \mathbf{e}* with respect to the bilinear form β . Both dual bases are uniquely determined by the following *orthogonality relations*:

$$\beta({}^\vee e_i, e_j) = \beta(e_i, e_j^\vee) = \begin{cases} 1 & \text{for } i = j, \\ 0 & \text{for } i \neq j, \end{cases} \quad (16.17)$$

and are expressed through \mathbf{e} as ${}^\vee \mathbf{e} = \mathbf{e} (B_e^t)^{-1}$ and $\mathbf{e}^\vee = \mathbf{e} B_e^{-1}$. Once one of the dual bases of \mathbf{e} is known, the coordinates of every vector $v \in V$ in the basis \mathbf{e} can be computed as the inner products of v with the dual basis vectors:

$$v = \sum_v \beta({}^\vee e_v, v) \cdot e_v = \sum_v \beta(v, e_v^\vee) \cdot e_v. \quad (16.18)$$

16.2.2 Isotropic Subspaces

A subspace $U \subset V$ is called *isotropic* for a bilinear form β if

$$\forall u, w \in U \quad \beta(u, w) = 0.$$

For example, the linear spans of the first n and of the last n standard basis vectors in \mathbb{k}^{2n} are isotropic for both the hyperbolic and symplectic forms on \mathbb{k}^{2n} considered in

¹⁴For details on exceptional bases of the Euler form over \mathbb{Z} , see [Problem 16.17](#) on p. 419.

Example 16.2 and Example 16.3 above. Note that all 1-dimensional subspaces are isotropic for all skew-symmetric forms.

Proposition 16.2 *The dimension of an isotropic subspace U of an arbitrary nondegenerate bilinear form on V is bounded above by the inequality.*

$$2 \dim U \leq \dim V$$

Proof A subspace $U \subset V$ is isotropic for β if and only if $\beta : V \rightarrow V^*$ sends U to $\text{Ann } U \subset V^*$. Since β is injective by the nondegeneracy assumption, $\dim U \leq \dim \text{Ann } U = \dim V - \dim U$. \square

Remark 16.1 Examples provided by symplectic and hyperbolic forms show that the upper bound from Proposition 16.2 is exact.

16.2.3 Isometry Group

Every isometric¹⁵ endomorphism $g : V \rightarrow V$ satisfies the relation $g^* \beta g = \beta$, which forces $\det^2 g \det \beta = \det \beta$. Since $\det \beta \neq 0$ for a nondegenerate form β , we conclude that $\det g = \pm 1$, and therefore g is invertible with $g^{-1} = \beta^{-1} g^* \beta$. The composition of isometries is clearly an isometry. Thus, all isometries of a given nondegenerate form β on V form a group. It is called the *isometry group*¹⁶ of β and is denoted by $O_\beta(V)$. Isometries of determinant 1 are called *special* and form a subgroup denoted by $SO_\beta(V) = O_\beta(V) \cap \text{SL}(V)$.

16.2.4 Correspondence Between Forms and Operators

A nondegenerate bilinear form β on V produces a linear isomorphism between the vector spaces of linear endomorphisms of V and bilinear forms on V ,

$$\text{End } V \xrightarrow{\sim} \text{Hom}(V, V^*), \quad f \mapsto \beta f, \quad (16.19)$$

which sends a linear operator $f : V \rightarrow V$ to the bilinear form $\beta f(u, w) = \beta(u, fw)$. The inverse isomorphism takes the correlation $\psi : V \rightarrow V^*$ to the endomorphism $f = \beta^{-1} \psi : V \rightarrow V$. The isomorphism (16.19) establishes a bijection between invertible operators and nonsingular bilinear forms.

¹⁵See formula (16.3) on p. 388.

¹⁶Or *orthogonal group* of β .

16.2.5 Canonical Operator

The operator $\kappa = \beta^{-1}\beta^* : V \rightarrow V$ corresponding to the left correlation β^* under the isomorphism (16.19) is called the *canonical* or *Serre* operator of the nondegenerate bilinear form β . It is uniquely determined by the condition

$$\forall u, w \in V, \quad \beta(w, u) = \beta(u, \kappa w). \quad (16.20)$$

We write κ_β for the canonical operator of β when a precise reference to β is required. In every basis of V , the matrix K of the canonical operator κ is expressed through the Gramian B of the form β as $K = B^{-1}B^t$.

Exercise 16.11 Check that under a transformation of a Gramian by the rule

$$B \mapsto C^t B C$$

for some $C \in \mathrm{GL}_n(\mathbb{k})$, the matrix $K = B^{-1}B^t$ of the canonical operator is transformed as $K \mapsto C^{-1}KC$.

Therefore, equivalent nondegenerate bilinear forms have similar canonical operators. Over an algebraically closed field of zero characteristic, the converse statement is true as well. In Theorem 16.1 on p. 401 below we will prove that over such a ground field, two nondegenerate bilinear forms are equivalent if and only if their canonical operators are similar. Thus, the classification of nondegenerate bilinear forms over an algebraically closed field of zero characteristic is completely reduced to the enumeration of all collections of elementary divisors $\mathcal{E}_\ell(\kappa)$ that the canonical operator of a nondegenerate bilinear form can have. We will do this in Theorem 16.3 on p. 407. Now let us mention some obvious constraints on $\mathcal{E}_\ell(\kappa)$.

Since $\beta(u, w) = \beta(w, \kappa u) = \beta(\kappa u, \kappa w)$ for all $u, w \in V$, the canonical operator is isometric. Up to a nonzero constant factor, the characteristic polynomial of the canonical operator

$$\chi_\kappa(t) = \det(tE - B^{-1}B^t) = \det^{-1}(B) \cdot \det(tB - B^t) = \det^{-1}(B) \cdot \chi_\beta(1, t)$$

coincides with the characteristic polynomial¹⁷ $\chi_\beta(t_0, t_1)$ of the form β expressed through the local affine coordinate $t = t_1/t_0$ on $\mathbb{P}_1 = \mathbb{P}(\Pi_\beta)$. Since $0, \infty$ are not among the characteristic values of a nondegenerate form, the eigenvalues of κ coincide with the characteristic values of β regarding their multiplicities. In particular, all eigenvalues of the canonical operator different from ± 1 split into inverse pairs λ, λ^{-1} of equal multiplicities.

Example 16.5 (Nondegenerate Form of Type $W_n(\lambda)$) For every $n \in \mathbb{N}$ and $\lambda \in \mathbb{k}^* = \mathbb{k} \setminus 0$, write $W_n(\lambda)$ for the even-dimensional coordinate space \mathbb{k}^{2n} equipped

¹⁷See Sect. 16.1.7 on p. 392.

with a bilinear form β whose Gramian in the standard basis has block form

$$B = \begin{pmatrix} 0 & E_n \\ J_n(\lambda) & 0 \end{pmatrix}, \quad (16.21)$$

where E_n and $J_n(\lambda)$ are the $n \times n$ identity matrix and the Jordan block¹⁸ of size n . The bilinear form β is nonsymmetric, nondegenerate, and has canonical operator

$$K = B^{-1}B^t = \begin{pmatrix} 0 & J_n^{-1}(\lambda) \\ E_n & 0 \end{pmatrix} \begin{pmatrix} 0 & J_n^t(\lambda) \\ E_n & 0 \end{pmatrix} = \begin{pmatrix} J_n^{-1}(\lambda) & 0 \\ 0 & J_n^t(\lambda) \end{pmatrix}.$$

Since the matrices $J_n^{-1}(\lambda)$ and $J_n^t(\lambda)$ are similar¹⁹ to $J_n(\lambda^{-1})$ and $J_n(\lambda)$ respectively, we conclude that

$$\mathcal{E}\ell(x) = \{(t - \lambda)^m, (t - \lambda^{-1})^m\}, \text{ where } \lambda \neq 0.$$

In other words, the Jordan normal form of x consists of two $n \times n$ blocks with nonzero inverse eigenvalues.

Example 16.6 (Nondegenerate Form of Type U_n) For $n \in \mathbb{N}$, write U_n for the coordinate space \mathbb{k}^n equipped with a bilinear form β whose Gramian in the standard basis is

$$B = \begin{pmatrix} & & & & & & 1 \\ & & & & & -1 & 1 \\ & & & & 1 & -1 & \\ & & \ddots & & \ddots & & \\ & (-1)^{n-2} & (-1)^{n-3} & \ddots & & & \\ (-1)^{n-1} & (-1)^{n-2} & & & & & \end{pmatrix} \quad (16.22)$$

(alternating ± 1 on the secondary diagonal and strictly below it; all other elements vanish). The canonical operator $K = B^{-1}B^t$ of this form is equal to

$$\begin{pmatrix} & & & & & & (-1)^{n-2} & (-1)^{n-1} \\ & & & & & (-1)^{n-3} & (-1)^{n-2} & \\ & & \ddots & & \ddots & & & \\ & -1 & 1 & & & & & \\ 1 & -1 & & & & & & \\ 1 & & & & & & & \end{pmatrix} \cdot \begin{pmatrix} & & & & & & (-1)^{n-1} \\ & & & & & (-1)^{n-2} & (-1)^{n-2} \\ & & \ddots & & \ddots & & \\ & 1 & 1 & & & & \\ -1 & -1 & & & & & \\ 1 & 1 & & & & & \end{pmatrix}$$

¹⁸See formula (15.9) on p. 375.

¹⁹See Exercise 15.21 on p. 383 and Exercise 15.6 on p. 365.

$$= (-1)^{n-1} \cdot \begin{pmatrix} 1 & 2 & 1 & & \\ & 1 & 2 & 1 & \\ & & \ddots & \ddots & \ddots \\ & & & 1 & 2 & 1 \\ & & & & 1 & 2 \\ & & & & & 1 \end{pmatrix}$$

and can be written as $(-1)^{n-1}E + 2N + N^2$, where N is a nilpotent operator with $N^n = 0$ and $N^{n-1} \neq 0$. If $\text{char } \mathbb{K} \neq 2$, then $M = 2N + N^2$ is also nilpotent with $M^n = 0$ and $M^{n-1} \neq 0$. Therefore, the Jordan normal form of K has exactly one block $J_n((-1)^{n-1})$ of size n with eigenvalue -1 for even n and $+1$ for odd n .

16.3 Adjoint Operators

Let V be a vector space with nondegenerate bilinear form β . Then associated with every linear operator $f : V \rightarrow V$ are the *right adjoint* operator $f^\vee : V \rightarrow V$ and *left adjoint* operator $f^\vee : V \rightarrow V$. The first of these is determined by the rule

$$\forall u, w \in V, \quad \beta(fu, w) = \beta(u, f^\vee w) \quad \text{or} \quad f^* \beta = \beta f^\vee, \quad (16.23)$$

which means commutativity of the following diagram:

$$\begin{array}{ccc} V^* & \xrightarrow{f^*} & V^* \\ \beta \uparrow & & \uparrow \beta \\ V & \xrightarrow{f^\vee} & V \end{array} \quad (16.24)$$

i.e., $f^\vee = \beta^{-1} f^* \beta$. The second operator ${}^\vee f : V \rightarrow V$ is determined by the symmetric prescription

$$\forall u, w \in V, \quad \beta({}^\vee f u, w) = \beta(u, fw) \quad \text{or} \quad ({}^\vee f)^* \beta = \beta f, \quad (16.25)$$

meaning the commutativity of the diagram

$$\begin{array}{ccc} V^* & \xrightarrow{f^*} & V^* \\ \beta^* \uparrow & & \uparrow \beta^* \\ V & \xrightarrow{{}^\vee f} & V \end{array} \quad (16.26)$$

i.e., ${}^\vee f = (\beta^*)^{-1} f^* \beta^*$. In every basis of V , the matrices ${}^\vee F$, F^\vee of the adjoint operators are expressed in terms of the matrix F of f and Gramian B of β as

$${}^\vee F = (B^t)^{-1} F^t B^t \quad \text{and} \quad F^\vee = B^{-1} F B. \quad (16.27)$$

Exercise 16.12 Show that ${}^\vee(f^\vee) = f = ({}^\vee f)^\vee$.

Both adjunction maps $f \mapsto f^\vee, f \mapsto {}^\vee f$ are *antihomomorphisms* with respect to the composition,

$$(fg)^\vee = g^\vee f^\vee \quad \text{and} \quad {}^\vee(fg) = {}^\vee g {}^\vee f,$$

because $\beta(fgu, w) = \beta(gu, f^\vee w) = \beta(u, g^\vee f^\vee w)$, $\beta(u, fgw) = \beta({}^\vee fu, gw) = \beta({}^\vee g {}^\vee fu, w)$.

Exercise 16.13 Show that the operator $g : V \rightarrow V$ is isometric if and only if g is invertible and ${}^\vee g = g^\vee = g^{-1}$.

Proposition 16.3 (Reflexivity) *For every vector space V with nondegenerate bilinear form β and linear operator $f : V \rightarrow V$, the following properties are equivalent:*

- (1) $f^{\vee\vee} = f$,
- (2) ${}^\vee{}^\vee f = f$,
- (3) ${}^\vee f = f^\vee$,
- (4) $\kappa_\beta f = f \kappa_\beta$,

where $\kappa_\beta = \beta^{-1} \beta^* : V \rightarrow V$ is the canonical operator²⁰ of β .

Proof By Exercise 16.12, the right adjunction of both sides in (3) leads to (1), from which (3) can be reobtained by left adjunction of both sides. For the same reason, (3) and (2) are equivalent as well. Property (3) can be written as $(\beta^*)^{-1} f^* \beta^* = \beta^{-1} f^* \beta$, which is equivalent to the equality $\beta (\beta^*)^{-1} f^* = f^* \beta (\beta^*)^{-1}$ between the operators on V^* . For the dual operators on V , we get the equality $f \beta^{-1} \beta^* = \beta^{-1} \beta^* f$, which is (4). \square

16.3.1 Reflexive Operators

A linear operator $f : V \rightarrow V$ is called *reflexive* with respect to a bilinear form β if it satisfies the equivalent conditions from Proposition 16.3. If a form β is either symmetric or skew-symmetric, then all linear endomorphisms of V are reflexive. For a nonsymmetric form β , the reflexive operators form a proper \mathbb{k} -subalgebra in

²⁰See Sect. 16.2.5 on p. 397.

$\text{End}(V)$, the centralizer of the canonical operator κ_β ,

$$Z(\kappa_\beta) \stackrel{\text{def}}{=} \{f \in \text{End}(V) \mid f\kappa_\beta = \kappa_\beta f\}.$$

Restricted to $Z(\kappa)$, the conjugation map $f \mapsto f^\vee = {}^\vee f$ becomes a linear involution. Therefore, $Z(\kappa)$ splits into a direct sum of ± 1 eigenspaces

$$Z(\kappa_\beta) = Z_+(\kappa) \oplus Z_-(\kappa), \text{ where } Z_\pm(\kappa) \stackrel{\text{def}}{=} \{f : V \rightarrow V \mid f^\vee = \pm f\}.$$

An operator $f : V \rightarrow V$ is called *self-adjoint* (respectively *anti-self-adjoint*) if $f^\vee = f$ (respectively $f^\vee = -f$). Equivalently, a self-adjoint operator f (respectively anti-self-adjoint operator q) is defined by the prescription

$$\forall u, w \in V \quad \beta(fu, w) = \beta(u, fw) \quad (\text{respectively } \beta(fu, w) = -\beta(u, fw)).$$

All (anti) self-adjoint operators are clearly reflexive. Therefore, the $Z_\pm(\kappa) \subset Z(\kappa)$ are exactly the subspaces of all (anti) self-adjoint operators. Every reflexive operator $f \in Z(\kappa) = Z_+(\kappa) \oplus Z_-(\kappa)$ uniquely splits as $f = f_+ + f_-$ for

$$f_+ \stackrel{\text{def}}{=} (f + f^\vee)/2 \in Z_+(\kappa) \text{ and } f_- \stackrel{\text{def}}{=} (f - f^\vee)/2 \in Z_-(\kappa).$$

Lemma 16.1 *Nondegenerate bilinear forms α, β on V have equal canonical operators $\kappa_\alpha = \kappa_\beta$ if and only if $\alpha = \beta f$ for some linear operator $f : V \rightarrow V$ that is self-adjoint with respect to both forms.*

Proof Let the canonical operators be equal, i.e., $\beta^{-1}\beta^* = \alpha^{-1}\alpha^*$. Dual to this equality is $\beta(\beta^*)^{-1} = \alpha(\alpha^*)^{-1}$. The operator $f = \beta^{-1}\alpha = (\beta^*)^{-1}\alpha^*$ commutes with $\kappa_\alpha = \kappa_\beta$, because $f\kappa_\alpha = \beta^{-1}\alpha^* = \kappa_\beta f$, and satisfies $\alpha = \beta f$. Conversely, if $\alpha = \beta f$ and f is self-adjoint with respect to β , i.e., $f = f^\vee = \beta^{-1}f^*\beta$, then $\kappa_\alpha = \alpha^{-1}\alpha^* = f^{-1}\beta^{-1}f^*\beta^* = f^{-1}f^\vee\beta^{-1}\beta^* = \beta^{-1}\beta^* = \kappa_\beta$. \square

Theorem 16.1 *Let the ground field \mathbb{K} be algebraically closed of zero characteristic. Then two nondegenerate bilinear forms are equivalent if and only if their canonical operators are similar.*

Proof Given a linear automorphism $g : V \xrightarrow{\sim} V$ such that $\alpha = g^*\beta g$, then

$$\kappa_\alpha = \alpha^{-1}\alpha^* = g^{-1}\beta^{-1}\beta^*g = g^{-1}\kappa_\beta g.$$

Conversely, let α and β have similar canonical operators $\kappa_\alpha = g^{-1}\kappa_\beta g$. Let us replace β by the equivalent correlation $g^*\beta g$. This allows us to assume that $\kappa_\beta = \kappa_\alpha$. Then by Lemma 16.1, $\alpha(u, w) = \beta(u, fw)$ for some nondegenerate operator $f : V \xrightarrow{\sim} V$ that is self-adjoint with respect to β . In Lemma 16.2 below, we construct²¹

²¹Under the assumption that the ground field is algebraically closed and has zero characteristic.

a polynomial $p(t) \in \mathbb{k}[t]$ such that the operator $h = p(f)$ satisfies $h^2 = f$. The operator h is also self-adjoint with respect to β , because $h^\vee = p(f)^\vee = p(f^\vee) = p(f) = h$. Since $\alpha(u, w) = \beta(u, fw) = \beta(u, h^2w) = \beta(hu, hw)$, the forms α and β are equivalent. \square

Lemma 16.2 *Over an algebraically closed field \mathbb{k} of characteristic zero, for every finite-dimensional nondegenerate operator f there exists a polynomial $p(t) \in \mathbb{k}[t]$ such that $p(f)^2 = f$.*

Proof Realize f as multiplication by t in the direct sum of residue modules of type $\mathbb{k}[t]/(t - \lambda)^m$, where $\lambda \neq 0$ by the assumption of the lemma. For each λ , write m_λ for the maximal exponent of binomials $(t - \lambda)^m$ appearing in the sum. Put $s = t - \lambda$ and consider the first m_λ terms of the formal power series expansion²²

$$\sqrt{t} = \sqrt{\lambda + s} = \lambda^{1/2} \cdot \sqrt{1 + \lambda^{-1/2}s} = \lambda^{1/2} + \frac{1}{2}s - \frac{\lambda^{-1/2}}{8}s^2 + \frac{\lambda^{-1}}{16}s^3 - \dots,$$

where $\lambda^{1/2} \in \mathbb{k}$ is either of the two roots of the quadratic equation $x^2 = \lambda$. Write $p_\lambda(t)$ for this sum considered as a polynomial in t . Then $p_\lambda^2(t) \equiv t \pmod{(t - \lambda)^{m_\lambda}}$. By the Chinese remainder theorem, there exists a polynomial $p(t) \in \mathbb{k}[t]$ such that $p(t) \equiv p_\lambda(t) \pmod{(t - \lambda)^{m_\lambda}}$ for all λ . Then $p^2 \equiv t \pmod{(t - \lambda)^{m_\lambda}}$ for each $\lambda \in \text{Spec}(f)$, that is, $p^2(f) = f$. \square

Remark 16.2 It follows from Theorem 16.1 that over an algebraically closed field of zero characteristic, for each $n \in \mathbb{N}$ there exist a unique, up to equivalence, nondegenerate symmetric bilinear form of dimension n and a unique, up to equivalence, nondegenerate skew-symmetric bilinear form of even dimension $2n$. Simple direct proofs of even stronger versions²³ of these claims will be given in Corollary 16.4 on p. 410 and Theorem 16.5 on p. 410 below.

Remark 16.3 If \mathbb{k} is not algebraically closed, Theorem 16.1 is not true even for symmetric forms. For example, over \mathbb{Q} there is a vast set of inequivalent nondegenerate symmetric forms, and its description seems scarcely realizable at this time. The isometry classes of the symmetric bilinear forms over the fields \mathbb{R} and \mathbb{F}_p will be enumerated in Sect. 17.3 on p. 431.

²²See formula (4.29) on p. 86.

²³Assuming only the constraint $\text{char } \mathbb{k} \neq 2$ on the characteristic and algebraic closure in the first case and for an arbitrary ground field in the second.

16.4 Orthogonals and Orthogonal Projections

16.4.1 Orthogonal Projections

Let U be a subspace of a vector space V with bilinear form $\beta : V \times V \rightarrow \mathbb{k}$. We write

$${}^\perp U = \{v \in V \mid \forall u \in U \beta(v, u) = 0\}, \quad (16.28)$$

$$U^\perp = \{v \in V \mid \forall u \in U \beta(u, v) = 0\}, \quad (16.29)$$

for the *left* and *right orthogonals* to U . For symmetric and skew-symmetric forms, these two orthogonals coincide, whereas for a nonsymmetric form, they are usually distinct.

Proposition 16.4 *If $\dim V < \infty$ and β is nondegenerate, then for every subspace $U \subset V$, we have*

$$\dim {}^\perp U = \dim V - \dim U = \dim U^\perp \quad \text{and} \quad ({}^\perp U)^\perp = U = {}^\perp(U^\perp).$$

Proof The first pair of equalities hold because the left and right orthogonals are the preimages of the same space $\text{Ann } U \subset V^*$ of dimension²⁴ $\dim \text{Ann } U = \dim V - \dim U$ under the linear isomorphisms $\beta^*, \beta : V \simeq V^*$. Since U is a subspace of both spaces $({}^\perp U)^\perp, {}^\perp(U^\perp)$ and all three spaces have the same dimension, the second pair of equalities holds. \square

Proposition 16.5 *Let V be an arbitrary²⁵ vector space with bilinear form β , and let $U \subset V$ be a finite-dimensional subspace such that the restriction of β to U is nondegenerate. Then $V = U^\perp \oplus U = U \oplus {}^\perp U$, and for every vector $v \in V$, its projections v_U and ${}_U v$ on U respectively along U^\perp and along ${}^\perp U$ are uniquely determined by the conditions $\beta(u, v) = \beta(u, v_U)$ and $\beta(v, u) = \beta({}_U v, u)$ for all $u \in U$. For a basis u_1, u_2, \dots, u_m in U , these projections can be computed as*

$$v_U = \sum \beta({}^\vee u_i, v) \cdot u_i \quad \text{and} \quad {}_U v \in U = \sum \beta(v, u_i^\vee) \cdot u_i,$$

where ${}^\vee u_i$ and u_i^\vee are taken from the left and right dual bases²⁶ in U .

Proof For every $v \in V$, the existence of the decomposition $v = w + v_U$ with $w \in U^\perp, v_U \in U$ means the existence of a vector $v_U \in U$ such that $\beta(u, v) = \beta(u, v_U)$ for all $u \in U$, because the latter equality says that $v - v_U \in U^\perp$. The uniqueness of the decomposition $v = w + v_U$ means that the vector v_U is uniquely determined by v . If the restriction of β to U is nondegenerate, then for every $v \in V$, the linear form

²⁴See Proposition 7.3 on p. 162.

²⁵Not necessarily finite-dimensional.

²⁶See formula (16.17) on p. 395.

$\beta(v) : U \mapsto \mathbb{K}$, $u \mapsto \beta(u, v)$, is uniquely represented as an inner product from the right with some vector $v_U \in U$, which is uniquely determined by v . We conclude that for every v , there exists a unique $v_U \in U$ such that $\beta(u, v) = \beta(u, v_U)$ for all $u \in U$, as required. This proves that $V = U^\perp \oplus U$. Since $\beta({}^\vee u_i, v_U) = \beta({}^\vee u_i, v)$, the expansion of the vector v_U through the basis u_1, u_2, \dots, u_m in U by formula (16.18) on p. 395 is $v_U = \sum \beta({}^\vee u_i, v_U) \cdot u_i = \sum \beta({}^\vee u_i, v) \cdot u_i$. For the right orthogonal, the arguments are completely symmetric. \square

Corollary 16.1 *Let V be a finite-dimensional vector space with nondegenerate bilinear form β and let $U \subset V$ be a subspace such that the restriction of β to U is nondegenerate as well. Then the restrictions of β to both orthogonals U^\perp , ${}^\perp U$ are nondegenerate too. For every vector $v \in V$, its projection ${}_{U^\perp} v \in U^\perp$ along U in the decomposition $V = U^\perp \oplus U$ is equal to $v - v_U \in U^\perp$ and is uniquely determined by the equality $\beta(v, w'') = \beta({}_{U^\perp} v, w'')$ for all $w'' \in U^\perp$. Symmetrically, the projection $v_{\perp U} \in {}^\perp U$ of v onto ${}^\perp U$ along U in the decomposition $V = U \oplus {}^\perp U$ is equal to $v - v_U$ and is uniquely determined by the equality $\beta(w', v) = \beta(w', v_{\perp U})$ for all $w' \in {}^\perp U$.*

Proof For every $w'' \in U^\perp$ there exists some $v \in V$ such that $\beta(v, w'') \neq 0$. We use the decomposition $V = U^\perp \oplus U$ from Proposition 16.5 to write it as $v = {}_{U^\perp} v + v_U$, where ${}_{U^\perp} v = v - v_U \in U^\perp$. The orthogonality relation $\beta(v_U, w'') = 0$ forces $\beta({}_{U^\perp} v, w'') = \beta(v, w'') \neq 0$. This proves that the restriction of β to U^\perp is nondegenerate and $\beta(v, w'') = \beta({}_{U^\perp} v, w'')$ for all $w'' \in U^\perp$. By Proposition 16.5 applied to U^\perp in the role of U , the vector ${}_{U^\perp} v$ is the projection of v onto U^\perp along ${}^\perp(U^\perp) = U$ in the direct sum $V = {}^\perp(U^\perp) \oplus U^\perp = U \oplus U^\perp$. The case of the left orthogonal is completely symmetric. \square

Corollary 16.2 *Under the assumptions of Corollary 16.1, the restrictions on U^\perp and ${}^\perp U$ of the two projections along U in the decompositions*

$$U \oplus {}^\perp U = V = U^\perp \oplus U$$

establish the inverse isometric isomorphisms

$$\lambda : U^\perp \xrightarrow{\sim} {}^\perp U, \quad w \mapsto w_{\perp U} = w - w_U, \quad (16.30)$$

$$\varrho : {}^\perp U \xrightarrow{\sim} U^\perp, \quad w \mapsto {}^\perp_U w = w - {}_U w. \quad (16.31)$$

For all $v \in V$, the projections $v_{\perp U}$ and ${}_{U^\perp} v$ along U are sent to each other by these isometries.

Proof The projection (16.30) is isometric, because for all $w', w'' \in U^\perp$,

$$\begin{aligned} \beta(w'_{\perp U}, w''_{\perp U}) &= \beta(w' - {}_U w', w'' - {}_U w'') \\ &= \beta(w', w'') - \beta({}_U w', w'') - \beta(w' - {}_U w', {}_U w'') \\ &= \beta(w', w'') - \beta({}_U w', w'') - \beta(w'_{\perp U}, {}_U w'') = \beta(w', w''). \end{aligned}$$

The isometric property of the projection (16.31) is verified similarly. Since both projections $v \mapsto {}_U v$, $v \mapsto v_U$ act identically on U , for every $v \in V$ we have

$$({}_U^\perp v)^\perp_U = (v - v_U)^\perp_U = v - v_U - {}_U(v - v_U) = v - v_U - {}_U v + v_U = v - {}_U v = v^\perp_U.$$

A similar computation verifies the equality ${}_{U^\perp}(v^\perp_U) = {}_U^\perp v$. Thus, both λ and ϱ are isometric and swap the two projections $v^\perp_U \in {}^\perp U$ and ${}_U^\perp v \in U^\perp$ of every vector $v \in V$. This forces λ , ϱ to be inverse to each other. \square

16.4.2 Biorthogonal Direct Sums

Subspaces $U, W \subset V$ are called *biorthogonal* with respect to a bilinear form β if $\beta(u, w) = 0$ and $\beta(w, u) = 0$ for all $u \in U$, $w \in W$. A form β is called *decomposable* if V splits into a direct sum of two nonzero biorthogonal subspaces. Otherwise, β is called *indecomposable*. If β is nondegenerate and $V = U \oplus W$, where $U, W \subset V$ are biorthogonal, then both restrictions of β onto U , W are forced to be nondegenerate, and the Gramian of β in any basis compatible with the decomposition $V = U \oplus W$ takes the block diagonal form

$$B = \begin{pmatrix} B_U & 0 \\ 0 & B_W \end{pmatrix},$$

where B_U , B_W are the Gramians of the restricted forms β_U , β_W . Therefore, the canonical operator of β also decomposes into a direct sum of canonical operators of the restricted forms on the summands. Every finite-dimensional space with bilinear form is certainly a direct orthogonal sum of indecomposable spaces.

Exercise 16.14 Check that the $2k$ -dimensional space $W_k(\lambda)$ from Example 16.5 on p. 397 for $\lambda = (-1)^{k-1}$ decomposes into a biorthogonal direct sum of two subspaces U_k .

16.4.3 Classification of Nondegenerate Forms

Everywhere in this section we assume by default that the ground field \mathbb{k} is algebraically closed of zero characteristic. For a linear operator $f : V \rightarrow V$, we say that a sequence of vectors $0 = u_0, u_1, u_2, \dots, u_k \in V$ is a *Jordan chain*²⁷ of length k with eigenvalue λ for f if $f(u_v) = \lambda u_v + u_{v-1}$ for all $1 \leq v \leq k$. This means that

²⁷See Sect. 15.2.1 on p. 367.

the linear span U of vectors the u_1, u_2, \dots, u_k is f -invariant and the matrix of $f|_U$ in the basis u_1, u_2, \dots, u_k is the Jordan block²⁸ $J_k(\lambda)$.

Lemma 16.3 *Let $f : V \rightarrow V$ be an isometry of an arbitrary nondegenerate bilinear form β on V and let*

$$0 = u_0, u_1, u_2, \dots, u_\ell, \quad 0 = w_0, w_1, w_2, \dots, w_m,$$

be two Jordan chains for f with eigenvalues λ and μ respectively. If $\lambda\mu \neq 1$ or $\ell \neq m$, then these chains are totally biorthogonal. If $\lambda\mu = 1$ and $\ell = m$, then the biorthogonality relations $\beta(u_i, w_j) = \beta(w_i, u_j) = 0$ hold for all $i + j < \ell = m$.

Proof Since $\beta(u_i, w_j) = \beta(\kappa u_i, \kappa w_j) = \beta(\lambda u_i + u_{i-1}, \mu w_j + w_{j-1})$, for all $1 \leq i \leq \ell$ and $1 \leq j \leq m$ we have the following recurrence relation:

$$(1 - \lambda\mu)\beta(u_i, w_j) = \lambda\beta(u_i, w_{j-1}) + \mu\beta(u_{i-1}, w_j) + \beta(u_{i-1}, w_{j-1}). \quad (16.32)$$

For $\lambda\mu \neq 1$, this implies by increasing induction²⁹ on $i + j$ that $\beta(u_i, w_j) = 0$ for all i, j . For $\lambda\mu = 1$, the equality (16.32) becomes the relation

$$\lambda\beta(u_i, w_{j-1}) + \mu\beta(u_{i-1}, w_j) + \beta(u_{i-1}, w_{j-1}) = 0.$$

The same increasing induction on $i + j$ shows that for every fixed $i + j = k < \max(\ell, m)$, the equality $\lambda\beta(u_i, w_{j-1}) = -\mu\beta(u_{i-1}, w_j)$ holds for all i, j with $i + j = k$. If $\ell \geq m$, then increasing induction on i shows that $\beta(u_i, w_j) = 0$ for all $i + j = k < \ell$. For $\ell \leq m$, increasing induction on j shows that $\beta(u_i, w_j) = 0$ for all $i + j = k < m$. \square

Theorem 16.2 *Let $f : V \rightarrow V$ be an isometry of a nondegenerate indecomposable bilinear form β on V . Then $\mathcal{E}\ell(f)$ consists either of k binomials $(t-1)^m$ with common $m = \dim V/k$ or of k binomials $(t+1)^m$ with common $m = \dim V/k$ or of k pairs of binomials $(t-\lambda)^m, (t-\lambda^{-1})^m$ with common $m = \dim V/(2k)$ and common $\lambda \neq \pm 1$.*

Proof Fix some Jordan basis \mathbf{e} for f , and for each $\lambda \in \text{Spec} f$, write U_λ for the linear span of all Jordan chains of maximal length with eigenvalue λ in \mathbf{e} . By Lemma 16.3, V splits into a direct biorthogonal sum $v = W \oplus W'$, where $W = U_\lambda + U_{\lambda^{-1}}$ and W' is the linear span of all the other Jordan chains in \mathbf{e} , which either have different eigenvalues or are shorter. Since β is indecomposable, we conclude that $W' = 0$, $V = U_\lambda + U_{\lambda^{-1}}$, and $\text{Spec}(f) = \{\lambda, \lambda^{-1}\}$. If $\lambda = \pm 1$, then $V = U_\lambda = U_{\lambda^{-1}}$, and the theorem holds. If $\lambda \neq \pm 1$, then $V = U_\lambda \oplus U_{\lambda^{-1}}$, and Lemma 16.3 forces both summands to be isotropic and to have the same length of Jordan chains spanning them. By Proposition 16.2 on p. 396, each summand has dimension at most $\frac{1}{2} \dim V$. This forces $\dim U_\lambda = \dim U_{\lambda^{-1}} = \frac{1}{2} \dim V$. Therefore, all Jordan chains in \mathbf{e} can be combined in pairs with equal lengths and inverse eigenvalues. \square

²⁸See Corollary 15.11 on p. 376.

²⁹The induction begins with $i + j = 0$ and $u_0 = w_0 = 0$.

Theorem 16.3 *Over an algebraically closed field of zero characteristic, a finite collection of possibly repeated binomials $(t-\lambda)^m$ with some $\lambda \in \mathbb{k}$, $m \in \mathbb{N}$ is realized as a collection of elementary divisors of the canonical operator of a nondegenerate bilinear form if and only if this collection satisfies the following four conditions: (1) all λ are nonzero; (2) all divisors with $\lambda \neq \pm 1$ are split into disjoint pairs with equal exponents m and inverse roots λ, λ^{-1} ; (3) for each even m , the number of divisors $(t-1)^m$ is even; (4) for each odd m , the number of divisors $(t+1)^m$ is even.*

Proof Let a collection of elementary divisors $(t-\lambda)^m$ satisfy conditions (1)–(4). Then it consists of some disjoint pairs of the form $(t-\lambda)^m, (t-\lambda^{-1})^m$, where repeated pairs are allowed, and some unpaired divisors $(t+1)^{2k}, (t-1)^{2k+1}$ whose exponents do not repeat. Each pair $(t-\lambda)^m, (t-\lambda^{-1})^m$ can be realized as a collection of elementary divisors of the canonical operator on the space³⁰ $W_m(\lambda)$. Each divisor $(t+1)^{2k}$ (respectively $(t-1)^{2k+1}$) can be realized as an elementary divisor of the canonical operator on the space³¹ U_{2k} (respectively U_{2k+1}). The total collection is realized in the biorthogonal direct sum of these spaces. Thus, conditions (1)–(4) are sufficient.

Let us verify that they are necessary. It is enough to check that conditions (1)–(4) hold for every indecomposable nondegenerate form. Since the canonical operator is isometric, we can apply Theorem 16.2. It says that $\text{Spec } \kappa$ is either $\{+1\}$ or $\{-1\}$ or $\{\lambda, \lambda^{-1}\}$ for some $\lambda \neq \pm 1$, and in the latter case, the elementary divisors of κ split into pairs with equal exponents and inverse roots. Therefore, conditions (1), (2) are necessary. Now assume $\text{Spec } \kappa = \{\varepsilon\}$, where $\varepsilon = \pm 1$. By Theorem 16.2, the Jordan basis of κ consists of k Jordan chains of the same length m . Therefore, $\kappa = \varepsilon \text{Id} + \eta$, where η is a nilpotent operator with $\eta^m = 0$ and

$$\dim \text{im } \eta^{m-1} = \dim(V / \ker \eta^{m-1}) = k.$$

Let $W = V / \ker \eta^{m-1}$. The orthogonality relations from Lemma 16.3 on p. 406 imply that $\text{im } \eta^{m-1}$ is biorthogonal to $\ker \eta^{m-1}$.

Exercise 16.15 Check this.

Hence, there is a bilinear form α on W well defined by $\alpha([u], [w]) \stackrel{\text{def}}{=} \beta(u, \eta^{m-1}w)$, where $u, w \in V$ and $[u], [w] \in W$ mean their classes modulo $\ker \eta^{m-1}$. This form is nondegenerate, because for every class $[w] \neq 0$, the vector $\eta^{m-1}w$ is nonzero, and therefore $\beta(u, \eta^{m-1}w) \neq 0$ for some $u \in V$. On the other hand, $\text{im } \eta^{m-1} = \ker \eta = \ker(\kappa - \varepsilon \text{Id})$ consists of eigenvectors of κ , which all have eigenvalue ε . Therefore, the form α can be written as

$$\alpha([u], [w]) = \beta(u, \eta^{m-1}w) = \beta(\kappa^{-1}\eta^{m-1}w, u) = \varepsilon\beta(\eta^{m-1}w, u).$$

The operator adjoint to η is $\eta^\vee = (\kappa - \varepsilon \text{Id})^\vee = \kappa^{-1} - \varepsilon \text{Id} = (\varepsilon \text{Id} + \eta)^{-1} - \varepsilon \text{Id} = \varepsilon((\text{Id} + \varepsilon\eta)^{-1} - \text{Id}) = -\eta + \varepsilon\eta^2 - \varepsilon\eta^3 + \dots$, which has $(\eta^\vee)^{m-1} = (-1)^{m-1}\eta^{m-1}$.

³⁰See 16.21 on p. 398.

³¹See 16.22 on p. 398.

Hence

$$\begin{aligned}\alpha([u], [w]) &= \varepsilon\beta(\eta^{m-1}w, u) = \varepsilon\beta\left(w, (\eta^\vee)^{m-1}u\right) \\ &= (-1)^{m-1}\varepsilon\beta(w, \eta^{m-1}u) = (-1)^{m-1}\varepsilon\alpha(w, u).\end{aligned}$$

Thus for $\varepsilon = (-1)^m$, the nondegenerate form α on W is skew-symmetric. This forces $\dim W$ to be even by [Exercise 16.9](#) on p. 394. Hence the numbers of Jordan chains with even length m and eigenvalue $+1$ and with odd length m and eigenvalue -1 both should be even; that is, conditions (3), (4) are necessary too. \square

Corollary 16.3 *Over an algebraically closed field of zero characteristic, all indecomposable finite-dimensional vector spaces with nondegenerate bilinear forms are exhausted up to isometry by the n -dimensional spaces U_n , $n \in \mathbb{N}$, from [Example 16.6](#) on p. 398, and the $2n$ -dimensional spaces $W_n(\lambda)$, $n \in \mathbb{N}$, $\lambda \neq (-1)^{n-1}$, from [Example 16.5](#) on p. 397. All these forms are inequivalent. \square*

16.5 Symmetric and Skew-Symmetric Forms

In this section, \mathbb{k} means any field of any characteristic. Recall³² that a bilinear form β on V is called *symmetric* if $\beta(v, w) = \beta(w, v)$ for all $v, w \in V$. This is equivalent to the conditions $\kappa_\beta = \text{Id}_V$, $\beta^* = \beta$, and $B^t = B$, where B is any Gramian of β .

A bilinear form is called *skew-symmetric* if $\beta(v, v) = 0$ for all $v \in V$. This definition implies what was given in Sect. 16.1.6 on p. 391, because the equalities

$$0 = \beta(u + w, u + w) = \beta(u, u) + \beta(w, w) + \beta(u, w) + \beta(w, u) = \beta(u, w) + \beta(w, u)$$

force $\beta(u, w) = -\beta(w, u)$. If $\text{char } \mathbb{k} \neq 2$, then both definitions are equivalent, and they mean that $\kappa_\beta = -\text{Id}_V$, $\beta^* = -\beta$, and $B^t = -B$, where B is any Gramian of β . However, for $\text{char } \mathbb{k} = 2$, the condition $\beta(u, w) = -\beta(w, u)$ becomes $\beta(u, w) = \beta(w, u)$, whereas the condition $\beta(v, v) = 0$ becomes more restrictive: it says that the Gramian B of a skew-symmetric form is symmetric with zeros on the main diagonal. In other words, for $\text{char } \mathbb{k} = 2$, the involution $\beta \mapsto \beta^*$ is not diagonalizable but is similar to multiplication by t in $\mathbb{k}[t]/((t+1)^2)$. The symmetric forms form the kernel of the nilpotent operator $\beta \mapsto \beta + \beta^*$, whereas the skew-symmetric forms form the image of this operator.

³²See Sect. 16.1.6 on p. 391.

16.5.1 Orthogonals and Kernel

Let β be either symmetric or skew-symmetric. Then the left and right orthogonals to every subspace $U \subseteq V$ coincide. This two-sided orthogonal is denoted by

$$U^\perp = \{w \in V \mid \forall u \in U \beta(u, w) = 0\}$$

and called just the *orthogonal* to U . In particular, the left and right kernels of β coincide:

$$V^\perp = V^\perp = \{w \in V \mid \forall v \in V \beta(v, w) = 0\}.$$

We call this space just the *kernel* of β and denote it by $\ker \beta$.

Proposition 16.6 *For every subspace $U \subset V$, complementary³³ to $\ker \beta$ the restriction to U of the (skew) symmetric form β is nondegenerate.*

Proof Let $u \in U$ satisfy $\beta(u, w) = 0$ for all $w \in U$. Since $V = U \oplus \ker \beta$, we can write every $v \in V$ as $v = w + e$, where $w \in U$ and $e \in \ker \beta$. Then $\beta(u, v) = \beta(u, w) + \beta(u, e) = 0$ for every $v \in V$. Hence, $w \in U \cap \ker \beta = 0$. \square

Caution 2 For a nonsymmetric bilinear form, Proposition 16.6 formulated for a one-sided kernel, whether a left kernel or a right kernel, is false.

16.5.2 Orthogonal Projections

If the restriction of a (skew) symmetric form β to a subspace $U \subset V$ is nondegenerate, then $V = U \oplus U^\perp$ by Corollary 16.1. In this case, the subspace U^\perp is called the *orthogonal complement* to U . The projection of the vector $v \in V$ onto U along U^\perp is denoted by $\pi_U v$ and called the *orthogonal projection*. It is uniquely determined by the relation $\beta(u, v) = \beta(u, \pi_U v)$ for all $u \in U$. If a (skew) symmetric form β is nondegenerate on all of V , then by Proposition 16.5, $\dim U^\perp = \dim V - \dim U$ and $U^{\perp\perp} = U$ for all subspaces $U \subset V$. By Corollary 16.1, the restriction of a nondegenerate form β onto a subspace $U \subset V$ is nondegenerate if and only if the restriction of β onto U^\perp is nondegenerate.

Theorem 16.4 (Lagrange's Theorem) *Let β be a symmetric bilinear form on a finite-dimensional vector space over an arbitrary field \mathbb{k} with $\text{char } \mathbb{k} \neq 2$. Then β has a diagonal Gramian in some basis.*

Proof Induction on $\dim V$. If $\dim V = 1$ or if β is zero, then the Gramian of β is diagonal in every basis. If $\beta \neq 0$, then there exists some vector $e \in V$ such that

³³That is, such that $V = U \oplus \ker \beta$.

$\beta(e, e) \neq 0$, because otherwise,

$$\beta(u, w) = (\beta(u + w, u + w) - \beta(u, u) - \beta(w, w))/2 = 0$$

for all $u, w \in V$. Since the restriction of β to a 1-dimensional subspace $U = \mathbb{k} \cdot e$ is nondegenerate, $V = U \oplus U^\perp$. By the inductive hypothesis, there is a basis with diagonal Gramian in U^\perp . Attaching the vector e to this basis, we get the required basis in V . \square

Corollary 16.4 *Two symmetric bilinear forms over an algebraically closed field \mathbb{k} with $\text{char}(\mathbb{k}) \neq 2$ are equivalent if and only if they have equal ranks.*³⁴

Proof Over an algebraically closed field, every nonzero diagonal element of the Gramian is equal to 1 after dividing the corresponding basis vector e_i by $\sqrt{\beta(e_i, e_i)}$. \square

Theorem 16.5 (Darboux's Theorem) *Over an arbitrary field,³⁵ every finite-dimensional vector space V with nondegenerate skew-symmetric form ω is equivalent to a symplectic space.³⁶ In particular, $\dim V$ is necessarily even.*

Proof We will construct a basis e_1, e_2, \dots, e_{2n} in V with block diagonal Gramian formed by 2×2 blocks

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (16.33)$$

After that, we reorder the basis vectors by writing first all vectors e_i with odd i and then all vectors e_i with even i . This gives the symplectic Gramian

$$\begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}.$$

Let $e_1 \in V$ be an arbitrary vector. Since ω is nondegenerate, there exists a vector $w \in V$ such that $\omega(e_1, w) = a \neq 0$. We put $e_2 = w/a$. Then the Gramian of (e_1, e_2) has the required form (16.33). Write $U \subset V$ for the linear span of e_1, e_2 . Since the Gramian of (e_1, e_2) has nonzero determinant, the vectors e_1, e_2 are linearly independent. Thus, $\dim U = 2$, and the restriction of ω to U is nondegenerate. Therefore, $V = U \oplus U^\perp$, and the restriction of ω to U^\perp is nondegenerate as well. Induction on $\dim V$ allows us to assume that U^\perp has a basis with the required block diagonal Gramian. We attach e_1, e_2 to this basis and get the required basis in V . \square

³⁴See Definition 16.1 on p. 391.

³⁵Of any characteristic.

³⁶See Example 16.3 on p. 393.

16.5.3 Adjoint Operators

Since the canonical operator of a nondegenerate (skew) symmetric form β belongs to the center of the algebra $\text{End } V$, every linear operator $f : V \rightarrow V$ is reflexive³⁷ for β . We write $f^\vee = \beta^{-1}f^*\beta$ for the (two-sided) operator adjoint to f . For all $u, w \in V$, it satisfies the equalities $\beta(u, f^\vee w) = \beta(fu, w)$ and $\beta(f^\vee u, w) = \beta(u, fw)$, which are equivalent to each other if β is (skew) symmetric. If $\text{char } \mathbb{k} \neq 2$, then the involution $f \mapsto f^\vee$ is diagonalizable, and $\text{End}(V) = \text{End}_+(V) \oplus \text{End}_-(V)$, where the ± 1 -eigenspaces

$$\begin{aligned}\text{End}_+(V) &\stackrel{\text{def}}{=} \{\varphi \in \text{End}(V) \mid f^\vee = f\} \\ \text{End}_-(V) &\stackrel{\text{def}}{=} \{\varphi \in \text{End}(V) \mid f^\vee = -f\}\end{aligned}$$

consist of *self-adjoint* and *anti-self-adjoint* operators, which satisfy for all $u, w \in V$ the equalities $\beta(fu, w) = \beta(u, fw)$ and $\beta(fu, w) = -\beta(u, fw)$ respectively.

16.5.4 Form–Operator Correspondence

For a nondegenerate symmetric form β on V , the linear isomorphism

$$\text{End}(V) \simeq \text{Hom}(V, V^*), \quad f \mapsto \beta f, \quad (16.34)$$

from Sect. 16.2.4 on p. 396 establishes linear isomorphisms between (anti)self-adjoint operators and (skew)symmetric correlations. For a nondegenerate *skew*-symmetric form β , the isomorphism (16.34) takes self-adjoint operators to skew-symmetric forms and anti-self-adjoint operators to symmetric forms.

16.6 Symplectic Spaces

We write Ω_{2n} for the $2n$ -dimensional symplectic space considered up to isometric isomorphism. A convenient coordinate-free realization of Ω_{2n} is provided by the direct sum

$$W = U \oplus U^*, \quad \dim U = n, \quad (16.35)$$

³⁷See Sect. 16.3.1 on p. 400.

equipped with the skew-symmetric form

$$\omega((u_1, \xi_1), (u_2, \xi_2)) \stackrel{\text{def}}{=} \langle u_1, \xi_2 \rangle - \langle u_2, \xi_1 \rangle. \quad (16.36)$$

For every pair of dual bases e_1, e_2, \dots, e_n and $e_1^*, e_2^*, \dots, e_n^*$ in U and U^* , the vectors

$$e_1, e_2, \dots, e_n, e_1^*, e_2^*, \dots, e_n^*$$

form a symplectic basis in W ; i.e., their Gramian is

$$J = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}. \quad (16.37)$$

Exercise 16.16 Check that $\Omega_{2m} \oplus \Omega_{2k}$ is isometric to $\Omega_{2(m+k)}$.

16.6.1 Symplectic Group

The isometries $F : W \rightarrow W$ of a nondegenerate skew-symmetric form ω on a $2n$ -dimensional space W are called *symplectic operators*. They form a group, denoted by $\text{Sp}_\omega(W)$ and called the *symplectic group* of W with respect to the form ω . The matrices of symplectic operators written in an arbitrary symplectic basis of W form the *group of symplectic matrices*

$$\text{Sp}_{2n}(\mathbb{k}) \stackrel{\text{def}}{=} \{F \in \text{Mat}_{2n}(\mathbb{k}) \mid F^t \cdot J \cdot F = J\}.$$

In the coordinate-free realization (16.35), every operator F on $W = U \oplus U^*$ can be written in block form

$$F = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where $A : U \rightarrow U$, $B : U^* \rightarrow U$, $C : U \rightarrow U^*$, $D : U^* \rightarrow U^*$. Then the symplectic condition $F^t \cdot J \cdot F = J$ becomes an equality:

$$\begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} = \begin{pmatrix} A^t & C^t \\ B^t & D^t \end{pmatrix} \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} -C^t A + A^t C & -C^t B + A^t D \\ -D^t A + B^t C & -D^t B + B^t D \end{pmatrix},$$

which is equivalent to the relations $C^t A = A^t C$, $D^t B = B^t D$, $E + C^t B = A^t D$. These show that there is an injective group homomorphism

$$\mathrm{GL}(U) \hookrightarrow \mathrm{Sp}_\omega(U^* \oplus U), \quad G \mapsto \begin{pmatrix} G & 0 \\ 0 & (G^t)^{-1} \end{pmatrix}.$$

16.6.2 Lagrangian Subspaces

Let V be a symplectic space of dimension $2n$ with symplectic form ω . The isotropic subspaces $L \subset V$ of maximal dimension $\dim L = n$ are called *Lagrangian subspaces*.

Proposition 16.7 *Every isotropic subspace $U \subset V$ is contained in some symplectic subspace $W \subset V$ of dimension $\dim W = 2 \dim U$. Every basis of U can be extended to some symplectic basis of W .*

Proof Chose a basis u_1, u_2, \dots, u_m in U , extend it to some basis in V , and write $u_1^\vee, u_2^\vee, \dots, u_m^\vee$ for the first m vectors of the dual basis with respect to ω . Therefore,

$$\omega(u_i, u_j^\vee) = \begin{cases} 1 & \text{for } i = j, \\ 0 & \text{for } i \neq j. \end{cases} \quad (16.38)$$

These relations will remain valid when we add to each u_j^\vee a linear combination of vectors u_i . Let us replace each u_j^\vee by a vector

$$w_j = u_j^\vee - \sum_{v < j} \omega(u_j^\vee, u_v^\vee) \cdot u_v. \quad (16.39)$$

Then we get vectors w_1, w_2, \dots, w_m satisfying the same orthogonality relations (16.38) and spanning an isotropic subspace, because for all $1 \leq i, j \leq m$,

$$\omega(w_i, w_j) = \omega(u_i^\vee, u_j^\vee) - \omega(u_j^\vee, u_i^\vee) \cdot \omega(u_i^\vee, u_i) = 0.$$

Therefore, the vectors u_i and w_j for $1 \leq i, j \leq m$ form a symplectic basis in their linear span. It remains to denote the latter by W . \square

Theorem 16.6 *For every Lagrangian subspace $L \subset V$, there exists a Lagrangian subspace $L' \subset V$ such that $V = L \oplus L'$. For every basis \mathbf{e} in L , there exists a unique basis \mathbf{e}' in L' such that the $2n$ vectors \mathbf{e}, \mathbf{e}' form a symplectic basis in V . For fixed L' , all Lagrangian subspaces L'' complementary to L are in bijection with the linear maps $f : L' \rightarrow L$ that are anti-self-adjoint with respect to ω .*

Proof If we repeat the proof of Proposition 16.7 for $U = L$ and $(u_1, u_2, \dots, u_m) = \mathbf{e}$, then we get $W = V = L \oplus L'$, where L' is spanned by the vectors w_j from (16.39).

This proves the first statement. To prove the second, we note that the correlation $\omega : V \xrightarrow{\sim} V^*$, $v \mapsto \omega(*, v)$, sends L' to the subspace $\omega(L') \subset V^*$, which is isomorphic to L^* . Let us identify $\omega(L')$ with L^* by means of this isomorphism. Then the basis w_1, w_2, \dots, w_n in L' , which extends e to a symplectic basis in V , is uniquely described as the preimage of the basis e^* in L^* dual to e . This proves the second statement. Every subspace $L'' \subset V = L \oplus L'$ complementary to L is mapped isomorphically onto L' by the projection along L . This means that for every $w \in L'$, there exists a unique vector $f(w) \in L$ such that $w + f(w) \in L''$. The assignment $w \mapsto f(w)$ produces a linear map $f : L' \rightarrow L$, whose graph is L'' . Since both subspaces L, L' are isotropic, for all $w_1, w_2 \in L'$ (with $f(w_1), f(w_2) \in L$), the equality $\omega(w_1 + f(w_1), w_2 + f(w_2)) = \omega(w_1, f(w_2')) + \omega(f(w_1), w_2)$ holds. Therefore, the subspace L'' , the graph of f , is isotropic if and only if for all $w_1, w_2 \in L'$,

$$\omega(w_1, f(w_2)) = -\omega(f(w_1), w_2) ,$$

which means that the map f is anti-self-adjoint with respect to ω . \square

16.6.3 Pfaffian

Consider the elements $\{a_{ij}\}_{i < j}$ of a skew-symmetric $(2n) \times (2n)$ matrix $A = (a_{ij})$ above the main diagonal as independent commutative variables and write $\mathbb{Z}[a_{ij}]$ for the ring of polynomials with integer coefficients in these variables. We are going to show that there exists a unique polynomial $\text{Pf}(A) \in \mathbb{Z}[a_{ij}]$ such that $\text{Pf}(A)^2 = \det(A)$ and $\text{Pf}(J') = 1$, where J' is the block diagonal matrix constructed from n identical 2×2 blocks

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} .$$

The polynomial $\text{Pf}(A)$ is called the *Pfaffian* of the skew-symmetric matrix A . We will show that it has the following explicit expansion through the matrix elements:

$$\text{Pf}(A) = \sum_{\substack{\{i_1, j_1\} \sqcup \dots \sqcup \{i_n, j_n\} = \\ = \{1, 2, \dots, 2n\}}} \text{sgn}(i_1 j_1 i_2 j_2 \dots i_n j_n) \cdot a_{i_1 j_1} a_{i_2 j_2} \dots a_{i_n j_n} , \quad (16.40)$$

where the summation ranges over all decompositions of the set $\{1, 2, \dots, 2n\}$ into a disjoint union of n pairs $\{i_\nu, j_\nu\}$ with $i_\nu < j_\nu$, and $\text{sgn}(g)$ means the sign of the

permutation $g \in S_{2n}$. For example,

$$\text{Pf} \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} = a, \quad \text{Pf} \begin{pmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{pmatrix} = af - be + cd.$$

It is convenient to put $a_{ij} \stackrel{\text{def}}{=} -a_{ji}$ for $i > j$ and consider $\{i_v, j_v\}$ in (16.40) as *unordered* pairs.

Exercise 16.17 Verify that:

- (a) The right-hand side of (16.40) is unchanged under transpositions within pairs (i_v, j_v) .
- (b) $\text{sgn}(i_1 j_1 i_2 j_2 \dots i_n j_n)$ does not depend on the order of the pairs.

Now we begin the construction of $\sqrt{\det A}$. Consider a matrix A , the Gramian of a skew-symmetric form ω on the coordinate vector space K^{2n} over the field $K = \mathbb{Q}(a_{ij})$ of rational functions in a_{ij} with coefficients in \mathbb{Q} . Since ω is nondegenerate, it follows from Theorem 16.5 that there exists a basis $e_1, e_1^*, e_2, e_2^*, \dots, e_n, e_n^*$ in K^{2n} with Gramian J' . Therefore, $A = C \cdot J' \cdot C^t$ for some matrix $C \in \text{GL}_{2n}(K)$. Hence, $\det(A) = \det(C)^2$, because $\det J' = 1$. It remains to check that $\det C$ coincides with the right-hand side of (16.40). To this end, we introduce another collection of commuting independent variables $\{b_{ij}\}_{1 \leq i < j \leq n}$, put $b_{ij} \stackrel{\text{def}}{=} -b_{ji}$ for $i > j$, and organize them all into a skew-symmetric matrix $B = (b_{ij})$. Consider the ring of Grassmannian polynomials in the skew-commuting variables $\xi = (\xi_1, \xi_2, \dots, \xi_n)$ with coefficients in the (quite huge) commutative ring $K[b_{ij}]$ and define there a homogeneous Grassmannian polynomial of degree 2 by

$$\beta_B(\xi) \stackrel{\text{def}}{=} (\xi B) \wedge \xi^t = \sum_{ij} b_{ij} \xi_i \wedge \xi_j.$$

Since even monomials $\xi_i \wedge \xi_j$ commute with each other, the n th power of $\beta_B(\xi)$ is equal to

$$\begin{aligned} \beta_B \wedge \beta_B \wedge \dots \wedge \beta_B &= n! \cdot \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_{2n} \\ &\times \sum_{\substack{\{i_1 j_1\} \sqcup \dots \sqcup \{i_n j_n\} \\ = \{1, 2, \dots, 2n\}}} \text{sgn}(i_1 j_1 i_2 j_2 \dots i_n j_n) \cdot b_{i_1 j_1} b_{i_2 j_2} \dots b_{i_n j_n}. \end{aligned} \tag{16.41}$$

The sum here is the same as in (16.40). Let us denote it by $\text{Pf}(B)$ and pass to new Grassmannian variables $\eta = (\eta_1, \eta_2, \dots, \eta_n)$ related to ξ by $\xi = \eta C$, where $C = \sqrt{\det A} \in \text{GL}_{2n}(K)$ is the same matrix as above. The right-hand side of (16.41) is now equal to

$$n! \cdot \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_{2n} \cdot \text{Pf}(B) = n! \cdot \det C \cdot \eta_1 \wedge \eta_2 \wedge \dots \wedge \eta_{2n} \cdot \text{Pf}(B).$$

On the other hand, the quadratic polynomial $\beta_B(\xi)$ under the substitution $\xi = \eta C$ is equal to

$$\beta_B(\xi) = (\xi B) \wedge \xi^t = (\eta CB) \wedge (\eta C)^t = (\eta CBC^t) \wedge \eta^t = \beta_{CBC^t}(\eta).$$

Therefore, the n th power of $\beta_B(\xi)$ is expanded through $\eta_1, \eta_2, \dots, \eta_n$ as

$$\beta_{CBC^t}(\eta) \wedge \beta_{CBC^t}(\eta) \wedge \dots \wedge \beta_{CBC^t}(\eta) = n! \cdot \eta_1 \wedge \eta_2 \wedge \dots \wedge \eta_{2n} \cdot \text{Pf}(CBC^t),$$

whence $\text{Pf}(CBC^t) = \text{Pf}(B) \cdot \det C$ in the ring $K[b_{ij}]$. Evaluating the variables b_{ij} by the substitution $B = J'$ leads to the equality $\text{Pf}(A) = \det C$ in the field $K = \mathbb{Q}(a_{ij})$. Hence $\sqrt{\det A} = \det C = \text{Pf}(A)$ can be computed by formula (16.40) and therefore lies in $\mathbb{Z}[a_{ij}]$. To prove that such a square root is unique, we note that the quadratic polynomial $x^2 - \det A = (x - \text{Pf}(A))(x + \text{Pf}(A)) \in \mathbb{Z}[a_{ij}][x]$ has just two roots, $x = \pm \text{Pf}(A)$, in the integral domain $\mathbb{Z}[a_{ij}]$. The normalization $\text{Pf}(J') = 1$ uniquely determines one of them.

Problems for Independent Solution to Chap. 16

Problem 16.1 Give an example of a vector space V with a nondegenerate bilinear form β and subspace $U \subset V$ such that the restriction of β to U is nondegenerate and $U^\perp \neq {}^\perp U$.

Problem 16.2 Give an example of a (nonsymmetric) correlation $\beta : V \rightarrow V^*$ and subspace $U \subset V$ such that $V = U \oplus \ker \beta$ and $U \cap \beta^{-1}(\text{Ann } U) \neq 0$.

Problem 16.3 Show that a bilinear form on V is regular³⁸ if and only if $V^\perp \cap V^\perp = 0$.

Problem 16.4 Show that for every nondegenerate indecomposable³⁹ bilinear form β , the symmetric part $\beta_+ = (\beta + \beta^*)/2$ or skew-symmetric part $\beta_- = \frac{(\beta - \beta^*)}{2}$ is nondegenerate⁴⁰ as well.

³⁸See Sect. 16.1.7 on p. 392.

³⁹See Sect. 16.4.2 on p. 405.

⁴⁰Compare with Exercise 16.7 on p. 391.

Problem 16.5 Show that for every linear operator f on a space with nondegenerate bilinear form, $\mathcal{E}\ell(f) = \mathcal{E}\ell(f^\vee) = \mathcal{E}\ell({}^\vee f)$.

Problem 16.6 (Reflexive Operators) Show that for every reflexive⁴¹ operator f on a space with nondegenerate bilinear form: (a) $\ker f^\vee = (\operatorname{im} f)^\perp = {}^\perp(\operatorname{im} f)$, (b) $\operatorname{im} f^\vee = (\ker f)^\perp = {}^\perp(\ker f)$.

Problem 16.7 (Normal Operators) A reflexive operator f on a space with nondegenerate bilinear form is called *normal* if $ff^\vee = f^\vee f$. Show that

- (a) (Anti) self-adjoint and isometric operators are normal.
- (b) for every normal operator f , both orthogonals $(\operatorname{im} f)^\perp$ and $(\ker f)^\perp$ are f -invariant.

Problem 16.8 (Isometries) Let f be an isometry of a nondegenerate bilinear form over an algebraically closed field \mathbb{k} with $\operatorname{char} \mathbb{k} \neq 2$. Show that f is similar to f^{-1} and use this to prove⁴² that all Jordan chains with eigenvalues $\lambda \neq \pm 1$ in any Jordan basis of f split into disjoint pairs of chains with equal lengths and inverse eigenvalues. Prove that there exists a Jordan basis for f in which the linear spans of these pairs of chains are biorthogonal to each other.

Problem 16.9 Show that the characteristic polynomial of every symplectic matrix $F \in \operatorname{Sp}_{2n}(\mathbb{k})$ is *reciprocal*, i.e., $\chi_F(t) = t^{2n} \chi_F(t^{-1})$. In particular, $\det F = 1$.

Problem 16.10 Show that every Lagrangian subspace L in a symplectic space coincides with L^\perp .

Problem 16.11 For all d in the range $1 \leq d \leq n$, show that the symplectic group $\operatorname{Sp}_\omega(\Omega_{2n})$ acts transitively on $2d$ -dimensional symplectic subspaces $W \subset \Omega_{2n}$ and on d -dimensional isotropic subspaces $U \subset \Omega_{2n}$.

Problem 16.12 Write an explicit expansion for the Pfaffian of a skew-symmetric 6×6 matrix.

Problem 16.13 Compute the 3-diagonal Pfaffian (all elements not shown are equal to zero)

$$\operatorname{Pf} \begin{pmatrix} 0 & a_1 & & & & \\ -a_1 & 0 & b_1 & & & \\ & -b_1 & \ddots & \ddots & & \\ & & \ddots & \ddots & b_{n-1} & \\ & & & -b_{n-1} & 0 & a_n \\ & & & & -a_n & 0 \end{pmatrix}.$$

⁴¹See Sect. 16.3.1 on p. 400.

⁴²Independently of Theorem 16.2.

Problem 16.14 For arbitrary $n \in \mathbb{N}$ and even $m \leq n$, consider an arbitrary skew-symmetric $n \times n$ matrix A and $m \times n$ matrix C . Prove that

$$\text{Pf}(CAC^t) = \sum_{\#I=m} \text{Pf}(A_{II}) \cdot \det(C_I),$$

where the summation is over all collections $I = (i_1, i_2, \dots, i_m)$ of strictly increasing indexes, and C_I, A_{II} denote square $m \times m$ submatrices situated in I -columns of C and in I -rows and I -columns of A .

Problem 16.15 Check that the canonical operator of the nonsymmetric Euler's form in Example 16.4 on p. 394 equals $T^{-n-1} = e^{-(n+1)D} : f(t) \mapsto f(t - n - 1)$. Use this to show that Euler's form is equivalent to U_{n+1} over \mathbb{Q} .

Problem 16.16 (Braid Group Action on Exceptional Bases) Let the vectors $e = (e_0, e_1, \dots, e_n)$ form an *exceptional*⁴³ basis for a nonsymmetric form β on V . Write L_i and R_i for the changes of basis that transform a pair of sequential vectors e_{i-1}, e_i by the rules

$$\begin{aligned} L_i : (e_{i-1}, e_i) &\mapsto (Le_i, e_{i-1}), \text{ where } Le_i = e_i - \beta(e_{i-1}, e_i) \cdot e_{i-1}, \\ R_i : (e_{i-1}, e_i) &\mapsto (e_i, Re_{i-1}), \text{ where } Re_{i-1} = e_{i-1} - \beta(e_{i-1}, e_i) \cdot e_i, \end{aligned}$$

and leave all the other basis vectors fixed. Show that the transformations L_i, R_i for $1 \leq i \leq n$ take an exceptional basis to an exceptional basis and satisfy the relations

$$\begin{aligned} L_i R_i &= R_i L_i = \text{Id}, \\ L_i L_{i+1} L_i &= L_{i+1} L_i L_{i+1} \quad \text{for all } 1 \leq i \leq n-1, \\ L_i L_j &= L_j L_i \quad \text{for } 1 \leq i, j \leq n \text{ and } |i-j| \geq 2. \end{aligned}$$

The group B_{n+1} presented by generators x_1, x_2, \dots, x_n and relators

$$(x_i x_{i+1})^3 \text{ for } 1 \leq i \leq n-1 \quad \text{and} \quad (x_i x_j)^2 \text{ for } 1 \leq i, j \leq n, |i-j| \geq 2$$

is called the *braid group of $n+1$ strands*. The symmetric group S_{n+1} can be constructed from B_{n+1} by adding n extra relators x_i^2 for $1 \leq i \leq n$. There is an open conjecture that any two exceptional bases of the Euler form from Example 16.4 on p. 394 can be transformed to each other by means of the action of the braid group, the action of the isometry group, and the action of the group

⁴³That is, with upper unitriangular Gramian B_e ; see Example 16.4 on p. 394.

$(\mathbb{Z}/(2))^{n+1}$ that multiplies basis vectors by ± 1 . This conjecture has been verified only for $n \leq 3$. The case $n = 2$ is considered in the next problem.

Problem 16.17 (Markov's Equation) Let $\beta_{\mathbb{C}} : \mathbb{C}^3 \times \mathbb{C}^3 \rightarrow \mathbb{C}$ be a nonsymmetric indecomposable bilinear form such that its restriction to $\mathbb{Z}^3 \subset \mathbb{C}^3$ takes integer values and has Gram determinant 1 in the standard basis of \mathbb{C}^3 . Write

$$\beta : \mathbb{Z}^3 \times \mathbb{Z}^3 \rightarrow \mathbb{Z}$$

for the restricted \mathbb{Z} -bilinear form. Convince yourself that \mathbb{C}^3 with the bilinear form $\beta_{\mathbb{C}}$ is isometrically isomorphic to the space $U_3(\mathbb{C})$ from Example 16.6 on p. 398. Check that β has Gram determinant 1 in every basis of \mathbb{Z}^3 over \mathbb{Z} .

(a) Let the Gramian of β in some basis \mathbf{u} of \mathbb{Z}^3 over \mathbb{Z} be upper unitriangular:

$$B_{\mathbf{u}} = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}.$$

Prove that $x = 3a$, $y = 3b$, $z = 3c$ for some $a, b, c \in \mathbb{Z}$ satisfying *Markov's equation*⁴⁴

$$a^2 + b^2 + c^2 = 3abc. \quad (16.42)$$

- (b) Verify that up to permutations, all positive solutions $(a, b, c) \in \mathbb{N}^3$ of the Markov equation (16.42) are obtained from $(1, 1, 1)$ by successive transformations⁴⁵ replacing a solution (a, b, c) either by $(3bc - a, b, c)$ or by $(a, 3ac - b, c)$ or by $(a, b, 3ab - c)$.
- (c) Prove that an exceptional basis⁴⁶ of \mathbb{Z}^3 over \mathbb{Z} can be transformed to some basis with Gramian⁴⁷

$$\begin{pmatrix} 1 & 3 & 6 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \quad (16.43)$$

by the action of the braid group B_3 described in Problem 16.16 and changing the directions of the basis vectors.

⁴⁴Hint: since $(\mathbb{C}^3, \beta_{\mathbb{C}})$ is isomorphic to U_3 , the canonical operator of β has $\text{tr } B_{\mathbf{u}}^{-1} B_{\mathbf{u}}^t = 3$.

⁴⁵They come from viewing equation (16.42) as a quadratic equation in one of variables a, b, c and replacing one known root by the other provided by Viète's formula.

⁴⁶That is, a basis with upper unitriangular Gramian.

⁴⁷Since the Gramian (16.43) coincides with the Gramian of the Euler form of rank 3, this verifies the conjecture from Problem 16.16 for rank-3 lattices. Moreover, we see that Euler's form of rank 3 is the unique integer bilinear form on \mathbb{Z}^3 that is indecomposable over \mathbb{C} and admits exceptional bases.

(d*) *Markov's conjecture* famously asserts that a triple of positive integer solutions of equation (16.42) is uniquely determined by its maximal element, i.e., for all positive integer solutions $a_1 \geq b_1 \geq c_1$ and $a_2 \geq b_2 \geq c_2$, the equality $a_1 = a_2$ forces $b_1 = b_2$ and $c_1 = c_2$. The question has remained open for more than a century.

Chapter 17

Quadratic Forms and Quadrics

Throughout this chapter, we assume that $\text{char } \mathbb{k} \neq 2$.

17.1 Quadratic Forms and Their Polarizations

17.1.1 Space with a Quadratic Form

Homogeneous quadratic polynomials¹ $q \in S^2 V^*$ over a vector space V are called *quadratic forms*. Every such polynomial may be considered a function $q : V \rightarrow \mathbb{k}$. A choice of basis $\mathbf{x} = (x_1, x_2, \dots, x_n)$ in V^* allows us to write q as

$$q(\mathbf{x}) = \sum_{i,j} q_{ij} x_i x_j, \quad (17.1)$$

where the summation is over all pairs of indices $1 \leq i, j \leq n$, and the coefficients are *symmetric*; i.e., they satisfy $q_{ij} = q_{ji}$. In other words, for $i \neq j$, both coefficients $q_{ji} = q_{ij}$ are equal to *half*² the coefficient of $x_i x_j$ in the reduced expansion of the polynomial $q \in \mathbb{k}[x_1, x_2, \dots, x_n]$ in terms of the monomials. The coefficients q_{ij} are organized in a symmetric $n \times n$ matrix $Q = (q_{ij})$. In matrix notation, the equality (17.1) becomes

$$q(\mathbf{x}) = \sum_{i,j} x_i q_{ij} x_j = \mathbf{x} Q \mathbf{x}^t, \quad (17.2)$$

¹See Sect. 11.2 on p. 258.

²Note that for $\text{char}(\mathbb{k}) = 2$, the representation (17.2) may be impossible.

where $\mathbf{x} = (x_1, x_2, \dots, x_n)$ means a row of variables, and \mathbf{x}^t is a transposed column. We see that a quadratic function $q : V \rightarrow \mathbb{k}$ can be written as $q(v) = \tilde{q}(v, v)$, where

$$\tilde{q} : V \times V \rightarrow \mathbb{k}, \quad \tilde{q}(\mathbf{x}, \mathbf{y}) = \mathbf{x}Q\mathbf{y}^t,$$

is a symmetric bilinear form with Gramian Q in the basis of V dual to \mathbf{x} . This bilinear form is called the *polarization* of the quadratic form q . It does not depend on the choice of basis and is uniquely determined by q as

$$\tilde{q}(u, w) = \frac{1}{2}(q(u + w) - q(u) - q(w)) = \frac{1}{4}(q(u + w) - q(u - w)). \quad (17.3)$$

Exercise 17.1 Check this and verify that in coordinates, $\tilde{q}(\mathbf{x}, \mathbf{y}) = \frac{1}{2} \sum_i y_i \frac{\partial q(\mathbf{x})}{\partial x_i}$.

Thus, for $\text{char } \mathbb{k} \neq 2$, the polarization of quadratic forms establishes the linear isomorphism

$$S^2 V^* \simeq \text{Hom}_+(V, V^*), \quad q \mapsto \tilde{q},$$

between homogeneous polynomials of degree 2 and symmetric bilinear forms on V . It allows us to transfer many notions related to symmetric bilinear forms to the world of quadratic forms. For example, a linear map $f : U_1 \rightarrow U_2$ between two spaces U_1, U_2 equipped with quadratic forms $q_1 \in S^2 U_1^*, q_2 \in S^2 U_2^*$ is isometric,³ that is, for all $u, w \in U_1$, it satisfies $\tilde{q}_1(u, w) = \tilde{q}_2(fu, fw)$ if and only if $q_1(u) = q_2(fu)$ for all $u \in U_1$. We call such maps *homomorphisms* of spaces with quadratic forms. Bijective homomorphisms are called *equivalences*⁴ of quadratic forms. Thus, a homomorphism of quadratic forms is nothing but a linear change of variables, and two quadratic forms are equivalent if one of them can be transformed to the other by an invertible linear change of variables. Classification of quadratic forms up to equivalence means the same as classification of symmetric bilinear forms up to isometry.

17.1.2 Gramian and Gram Determinant

The symmetric matrix Q in (17.2) is called the *Gramian*⁵ of the quadratic form q in the coordinates \mathbf{x} . It coincides with the Gramian of the bilinear form \tilde{q} in the basis $\mathbf{e} = (e_1, e_2, \dots, e_n)$ of V dual to $\mathbf{x} = (x_1, x_2, \dots, x_n)$, i.e., $q_{ij} = \tilde{q}(e_i, e_j)$. If bases \mathbf{x} and \mathbf{y} in V^* are related by $\mathbf{x} = \mathbf{y} \cdot C_{\mathbf{y}\mathbf{x}}$, then their Gramians $Q_{\mathbf{x}}, Q_{\mathbf{y}}$ satisfy the relation

³See Sect. 16.1 on p. 387.

⁴Or *isomorphisms*.

⁵Or *Gram matrix*.

$Q_y = C_{yx}Q_xC_{yx}^t$. Therefore, under a change of basis, the determinant of the Gram matrix is multiplied by the nonzero square $\det^2 C_{yx} \in \mathbb{k}$. We conclude that the class of $\det Q$ modulo multiplication by nonzero squares does not depend on the basis. We denote this class by $\det q \in \mathbb{k}/\mathbb{k}^{*2}$ and call it the *Gram determinant* of the quadratic form q . If $\det q = 0$, then the quadratic form q is called *singular*.⁶ Otherwise, q is called *nonsingular*.⁷ Let us write $a \sim b$ for $a, b \in \mathbb{k}$ such that $a = \lambda^2 b$ for some $\lambda \in \mathbb{k}^*$. If $\det q_1 \sim \det q_2$, then q_1 and q_2 are certainly inequivalent.

17.1.3 Kernel and Rank

Let us write $\hat{q} : V \rightarrow V^*$, $v \mapsto \tilde{q}(*, v)$ for the correlation map⁸ of the symmetric bilinear form \tilde{q} and call it the *correlation* of the quadratic form q . The correlation takes a vector $v \in V$ to the covector $u \mapsto \tilde{q}(u, v)$. We write

$$\ker q \stackrel{\text{def}}{=} \ker \hat{q} = \{v \in V \mid \forall u \in V \tilde{q}(u, v) = 0\}$$

for the kernel of the correlation and call it the *kernel* of the quadratic form q . A form q is nonsingular if and only if $\ker q = 0$. The number

$$\text{rk } q \stackrel{\text{def}}{=} \dim \text{im } \hat{q} = \dim V / \ker q$$

is called the *rank* of the quadratic form q . It coincides with the rank of the Gramian of q in any basis of V . Quadratic forms of different ranks certainly are inequivalent.

For a singular quadratic form q on V , we write q_{red} for the quadratic form on $V / \ker q$ defined by $q_{\text{red}}([v]) = q(v)$.

Exercise 17.2 Check that the form q_{red} is well defined and nondegenerate.

17.1.4 Sums of Squares

A basis in V is called *orthogonal* for q if q has a diagonal Gramian in this basis, i.e., is a linear combination of squares:

$$q(x) = a_1x_1^2 + a_2x_2^2 + \cdots + a_rx_r^2, \text{ where } r = \text{rk } q. \quad (17.4)$$

⁶Or *degenerate*.

⁷Or *nondegenerate*.

⁸See Sect. 16.1 on p. 387.

By Lagrange's theorem,⁹ every quadratic form admits an orthogonal basis over every field \mathbb{k} with $\text{char } \mathbb{k} \neq 2$. Note that the number of nonzero coefficients in (17.4) is equal to $\text{rk } q$ and therefore does not depend on the choice of orthogonal basis. If \mathbb{k} is algebraically closed, then the substitution $x_i \mapsto x_i/\sqrt{a_i}$ simplifies (17.4) to $q(\mathbf{x}) = x_1^2 + x_2^2 + \cdots + x_r^2$. Therefore, over an algebraically closed field \mathbb{k} of characteristic $\text{char } \mathbb{k} \neq 2$, two quadratic forms are equivalent if and only if they have equal ranks.

Example 17.1 (Binary Quadratic Forms) Quadratic forms in two variables are called *binary*. Every nonzero binary quadratic form

$$q(x) = ax_1^2 + 2bx_1x_2 + cx_2^2 = (x_1, x_2) \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

in appropriate coordinates t_1, t_2 becomes either αt_1^2 , where $\alpha \neq 0$, or $\alpha t_1^2 + \beta t_2^2$, where $\alpha, \beta \neq 0$. In the first case, $ac - b^2 \sim \det q \sim \alpha \cdot 0 = 0$, i.e., the form q is singular. It vanishes identically on the 1-dimensional subspace $\text{Ann}(t_1) \subset V$ and is nonzero everywhere outside it. In the second case, $ac - b^2 \sim \det q \sim \alpha\beta \neq 0$ and q is nonsingular. If there exists some $v = (\vartheta_1, \vartheta_2) \neq 0$ such that $q(v) = \alpha\vartheta_1^2 + \beta\vartheta_2^2 = 0$, then $-\det q \sim -\alpha\beta \sim -\beta/\alpha = (\vartheta_1/\vartheta_2)^2$ is a square¹⁰ in \mathbb{k} , and

$$q(t) = \alpha t_1^2 + \beta t_2^2 = \alpha \left(t_1 + \frac{\vartheta_1}{\vartheta_2} t_2 \right) \left(t_1 - \frac{\vartheta_1}{\vartheta_2} t_2 \right)$$

is a product of two different linear forms. It vanishes identically on two different 1-dimensional subspaces and is nonzero everywhere outside them.

Exercise 17.3 Show that \tilde{q} is a hyperbolic form¹¹ on \mathbb{k}^2 in this case.

If $-\det q$ is not a square, then $q(v) \neq 0$ for all $v \neq 0$. Such a form is called *anisotropic*.

17.1.5 Isotropic and Anisotropic Subspaces

A vector $v \neq 0$ is called *isotropic* for q if $q(v) = 0$. If $q(v) \neq 0$, then the vector v is called *anisotropic*. A subspace $U \subset V$ is called *anisotropic* if all nonzero $u \in U$ are anisotropic, i.e., if $q|_U$ vanishes only at zero. A form q is called *anisotropic* if the whole space V is anisotropic. For example, the Euclidean quadratic form $q(v) = |v|^2$ is anisotropic. We have seen in Example 17.1 that a 2-dimensional subspace

⁹See Theorem 16.4 on p. 409.

¹⁰Note that $\vartheta_1, \vartheta_2 \neq 0$, because $\alpha\vartheta_1^2 + \beta\vartheta_2^2 = 0$ and $v \neq 0$.

¹¹See Example 16.2 on p. 393.

U over a field \mathbb{k} with $\text{char } \mathbb{k} \neq 2$ is anisotropic if and only if $-\det(q|_U)$ is not a square in \mathbb{k} . In particular, if \mathbb{k} is algebraically closed, then there are no anisotropic subspaces of dimension ≥ 2 over \mathbb{k} .

A subspace $U \subset V$ is called *isotropic* for a quadratic form q if every vector $u \in U$ is isotropic, i.e., $q|_U \equiv 0$. In this case, formulas (17.3) imply that $\tilde{q}(u_1, u_2) = 0$ for all $u_1, u_2 \in U$. Thus, U is isotropic for a quadratic form q if and only if U is isotropic for the bilinear form \tilde{q} in the sense of Sect. 16.2.2 on p. 395. By Proposition 16.2, the dimensions of isotropic subspaces for a nonsingular quadratic form are bounded above by $\dim V/2$.

17.1.6 Hyperbolic Forms

Write H_{2n} for the $2n$ -dimensional hyperbolic space¹² considered up to isomorphism. A convenient coordinate-free realization of H_{2n} is the direct sum

$$H_{2n} = U \oplus U^*, \text{ where } \dim U = n,$$

equipped with the symmetric bilinear form $\tilde{h}(u_1 + \xi_1, u_2 + \xi_2) \stackrel{\text{def}}{=} \xi_1(v_2) + \xi_2(v_1)$, where $u_1, u_2 \in U$, $\xi_1, \xi_2 \in U^*$. Both summands U, U^* are isotropic. Mixed inner products of vectors and covectors are given by contractions: $\tilde{h}(\xi, v) = \tilde{h}(v, \xi) = \langle v, \xi \rangle$. Every basis of W arranged from dual bases

$$e_1, e_2, \dots, e_n, e_1^*, e_2^*, \dots, e_n^* \quad (17.5)$$

of U and U^* is *hyperbolic*, that is, has Gramian

$$\begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix},$$

where both the zero and identity blocks $0, E$ are of size $n \times n$. The vectors $\tilde{p}_i = e_i + e_i^*$ and $\tilde{q}_i = e_i - e_i^*$ form an orthogonal basis of \tilde{h} . Their inner squares are $\tilde{h}(\tilde{p}_i, \tilde{p}_i) = 2$ and $\tilde{h}(\tilde{q}_i, \tilde{q}_i) = -2$.

A quadratic form $h(v) = \tilde{h}(v, v)$ obtained from a bilinear form \tilde{h} also is called *hyperbolic*. It provides $h(u + \xi) = 2\xi(u)$. In coordinates \mathbf{x} with respect to the hyperbolic basis (17.5), a hyperbolic quadratic form looks like

$$h(\mathbf{x}) = 2x_1x_{n+1} + 2x_2x_{n+2} + \cdots + 2x_nx_{2n},$$

¹²See Example 16.2 on p. 393.

and after renaming $2x_i$ by x_i for $1 \leq i \leq n$, it becomes

$$x_1x_{n+1} + x_2x_{n+2} + \cdots + x_nx_{2n}.$$

In coordinates z with respect to the orthogonal basis $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_n$, it is

$$h(z) = 2z_1^2 + 2z_2^2 + \cdots + 2z_n^2 - 2z_{n+1}^2 - 2z_{n+2}^2 - \cdots - 2z_{2n}^2.$$

Exercise 17.4 Check that the orthogonal direct sum $H_{2k} \oplus H_{2m}$ is equivalent to $H_{2(k+m)}$.

Hyperbolic spaces are much like the symplectic spaces considered in Sect. 16.6 on p. 411. For example, there is a symmetric analogue of Proposition 16.7 on p. 413.

Proposition 17.1 *Let V be a vector space with nondegenerate symmetric bilinear form β . Then every isotropic subspace $U \subset V$ is contained in some hyperbolic subspace $W \subset V$ of dimension $\dim W = 2 \dim U$. Every basis of U can be extended to a hyperbolic basis of W .*

Proof Choose a basis u_1, u_2, \dots, u_m in U , extend it to a basis in V , and write $u_1^\vee, u_2^\vee, \dots, u_m^\vee$ for the first m vectors of the dual basis with respect to β . Therefore,

$$\beta(u_i, u_j^\vee) = \begin{cases} 1 & \text{for } i = j, \\ 0 & \text{for } i \neq j. \end{cases} \quad (17.6)$$

These relations remain valid if we add any linear combination of vectors u_i to any u_j^\vee . Replacing each u_j^\vee by the vector

$$w_j = u_j^\vee - \frac{1}{2} \sum_v \beta(u_j^\vee, u_v^\vee) u_v,$$

we get a collection of m vectors w_1, w_2, \dots, w_m satisfying the same orthogonality relations (16.38). The linear span of the vectors w_j is isotropic, because for all

$$\beta(w_i, w_j) = \beta(u_i^\vee, u_j^\vee) - \frac{1}{2} \beta(u_i^\vee, u_j^\vee) - \frac{1}{2} \beta(u_j^\vee, u_i^\vee) = 0 \quad 1 \leq i, j \leq m.$$

Thus, the vectors u_i and w_j for $1 \leq i, j \leq m$ form a hyperbolic basis of their linear span. It remains to denote the latter by W . \square

Theorem 17.1 *Every vector space V with nondegenerate symmetric bilinear form is an orthogonal direct sum $V = H_{2k} \oplus U$, where $H_{2k} \subset V$ is some hyperbolic subspace, $U = H_{2k}^\perp$ is anisotropic, and either of the two summands may vanish.*

Proof Induction on $\dim V$. If V is anisotropic (in particular, for $\dim V = 1$), there is nothing to prove. If there exists some isotropic nonzero vector $e \in V$, then by Proposition 17.1, e is contained in some hyperbolic plane H_2 . Since the form is nondegenerate in this plane, V splits into the orthogonal direct sum $V = H_2 \oplus H_2^\perp$. If $H_2^\perp = 0$, we are done. If not, then by the inductive hypothesis, $H_2^\perp = H_{2m} \oplus U$, where $U = H_{2m}^\perp$ is anisotropic. Therefore, $V = H_{2m+2} \oplus U$. \square

Corollary 17.1 *Every quadratic form q in appropriate coordinates is of the form*

$$x_1x_{i+1} + x_2x_{i+2} + \cdots + x_ix_{2i} + \alpha(x_{2i+1}, x_{2i+2}, \dots, x_r),$$

where $r = \text{rk}(q)$ and $\alpha(x) \neq 0$ for $x \neq 0$. \square

17.2 Orthogonal Geometry of Nonsingular Forms

17.2.1 Isometries

Let V be a finite-dimensional vector space equipped with a nonsingular quadratic form $q \in S^2V^*$ with polarization $\tilde{q} : V \times V \rightarrow \mathbb{k}$. Recall¹³ that a linear operator $f : V \rightarrow V$ is called *orthogonal* (or *isometric*) with respect to \tilde{q} if

$$\tilde{q}(fu, fw) = \tilde{q}(u, w) \quad \forall u, w \in V.$$

By formula (17.3) on p. 422, this condition is equivalent to $q(fv) = q(v)$ for all $v \in V$. We know from Sect. 16.2.3 on p. 396 that the isometries of \tilde{q} form a group. In the context of a quadratic form, this group is called the *orthogonal group* of the nonsingular quadratic form q and is denoted by

$$\text{O}_q(V) = \{f \in \text{GL}(V) \mid \forall v \in V \, q(fv) = q(v)\}.$$

Example 17.2 (Isometries of the Hyperbolic Plane) Let the linear operator $f : H_2 \rightarrow H_2$ have matrix $F = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in a hyperbolic basis e, e^* of H_2 . Then F is orthogonal if and only if

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 2ac & ad + bc \\ ad + bc & 2bd \end{pmatrix},$$

¹³See Sect. 16.2.3 on p. 396.

i.e., when $ac = bd = 0$, $ad + bc = 1$. This system of equations has two families of solutions:

$$F_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \quad \text{and} \quad \widetilde{F}_\lambda = \begin{pmatrix} 0 & \lambda \\ \lambda^{-1} & 0 \end{pmatrix}, \quad \text{where } \lambda \text{ runs through } \mathbb{k}^*. \quad (17.7)$$

For $\mathbb{k} = \mathbb{R}$, the operator F_λ with $\lambda > 0$ is called a *hyperbolic rotation*, because the trajectory $F_\lambda v$ of every vector $v = (x, y)$ as λ runs through the open ray $(0, \infty)$ is a hyperbola $xy = \text{const.}$ If we put $\lambda = e^t$ and pass to an orthonormal basis $p = (e + e^*)/\sqrt{2}$, $q = (e - e^*)/\sqrt{2}$, the operator F_λ acquires the matrix

$$\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \cdot \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{pmatrix},$$

which looks quite similar to the matrix of Euclidean rotation. For $\lambda < 0$, the operator F_λ is a composition of a hyperbolic rotation with the central symmetry with respect to the origin. In both cases, F_λ are proper and preserve oriented areas, i.e., lie in $\text{SL}(\mathbb{R}^2)$. The operators \widetilde{F}_λ are not proper and can be decomposed as hyperbolic rotations followed by reflection in an axis of the hyperbola. They preserve Euclidean area¹⁴ but reverse the orientation.

17.2.2 Reflections

As in Euclidean geometry,¹⁵ every anisotropic vector $e \in V$ provides V with an orthogonal decomposition $V = \mathbb{k} \cdot e \oplus e^\perp$, where $e^\perp = \{v \in V \mid \tilde{q}(e, v) = 0\}$ is the *orthogonal hyperplane* of e . Associated with this decomposition is the *reflection* in the hyperplane e^\perp defined by

$$\sigma_e : V \rightarrow V, \quad v \mapsto \sigma_e(v) \stackrel{\text{def}}{=} v - 2 \frac{\tilde{q}(e, v)}{\tilde{q}(e, e)} \cdot e. \quad (17.8)$$

It acts identically on e^\perp and takes e to $-e$ (see Fig. 17.1). Therefore, $\sigma_e \in \text{O}_q$ and $\sigma_e^2 = 1$.

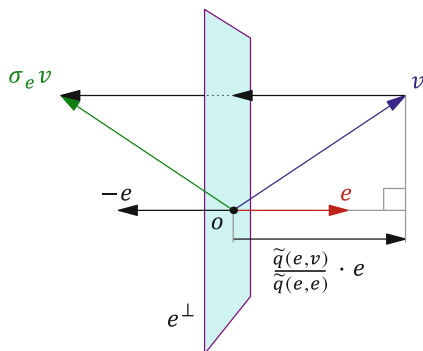
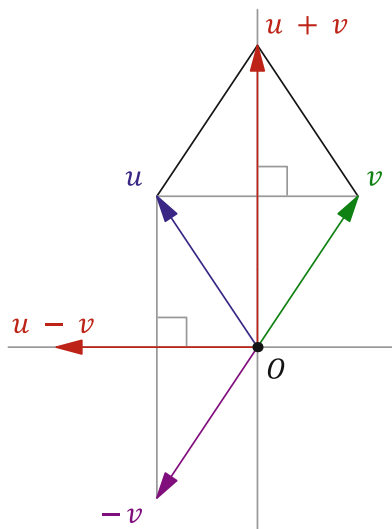
Exercise 17.5 Verify the equality

$$f \circ \sigma_e \circ f^{-1} = \sigma_{f(e)}$$

for every isometry $f : V \rightarrow V$ and anisotropic vector $e \in V$.

¹⁴That is, the absolute value of the oriented area.

¹⁵See Example 10.12 on p. 246.

Fig. 17.1 Reflection σ_e **Fig. 17.2** Reflections in a rhombus

Lemma 17.1 *In a space with a nonsingular quadratic form q , for every pair of anisotropic vectors u, w such that $q(u) = q(w)$, there exists a reflection that sends u either to w or to $-w$.*

Proof If u, w are collinear, then the reflection $\sigma_w = \sigma_u$ sends them to each other. Let u, w span the 2-dimensional plane U . The two diagonals of the rhombus spanned by u, v are $u+w$ and $u-v$. They are perpendicular: $\tilde{q}(u+v, u-v) = q(u) - q(v) = 0$. Since U is not isotropic for q , at least one of the two diagonals, which form an orthogonal basis in U , has to be anisotropic.¹⁶ Therefore, at least one of the two reflections in the diagonals is well defined (see Fig. 17.2). The reflection σ_{u-w} takes u to w ; the reflection σ_{u+w} takes u to $-w$. \square

¹⁶Otherwise, the Gram matrix of the basis formed by the diagonals is zero.

Exercise 17.6 Verify the last two statements and show that if V is anisotropic, then there exists a reflection that sends u exactly to w .

Theorem 17.2 *Every isometry of an n -dimensional space with a nonsingular symmetric form is a composition of at most $2n$ reflections in hyperplanes.*

Proof Induction on n . For $n = 1$, the orthogonal group of the anisotropic line consists of the identity E and reflection $-E$, because the linear map $v \mapsto \lambda v$ satisfying $q(v) = q(\lambda v) = \lambda^2 q(v)$ has $\lambda = \pm 1$. Now let $f : V \rightarrow V$ be an isometry of an n -dimensional space for $n > 1$. Choose any anisotropic vector v in V and write $\sigma : V \rightarrow V$ for the reflection that sends $f(v)$ either to v or to $-v$. The composition σf maps $v \mapsto \pm v$, and in both cases, sends the hyperplane v^\perp to itself. By the inductive hypothesis, the restriction of σf to v^\perp is a composition of at most $2(n-1)$ reflections within v^\perp . All these reflections can be considered reflections of V in hyperplanes containing the vector v . Then the composition of these $2n-2$ reflections of V equals either σf or $\sigma_v \sigma f$. Therefore, f , which equals either $\sigma(\sigma f)$ or $\sigma_v(\sigma_v \sigma f)$, is a composition of at most $(2n-2) + 2 = 2n$ reflections. \square

Exercise 17.7 Show that every isometry of an anisotropic space V is a composition of at most $\dim V$ reflections in hyperplanes.

Lemma 17.2 (Witt's Lemma) *Let U, V, W be spaces with nonsingular symmetric bilinear forms. If the orthogonal direct sum $U \oplus V$ is isometrically isomorphic to the orthogonal direct sum $U \oplus W$, then V and W are isometrically isomorphic.*

Proof Induction on $\dim U$. If $\dim U = 1$, then $U = \mathbb{k} \cdot u$, where u is anisotropic. Write

$$f : \mathbb{k} \cdot u \oplus V \xrightarrow{\sim} \mathbb{k} \cdot u \oplus W$$

for the isometric isomorphism in question. Let σ be the reflection of the second space such that $\sigma(f(u)) = \pm u$. Then the composition σf maps $u^\perp = V$ to $^{17}u^\perp = W$, as required. For $\dim U > 1$, we choose some anisotropic vector $u \in U$ and apply the inductive hypothesis to the orthogonal decompositions $U \oplus V = \mathbb{k} \cdot u \oplus (u^\perp \oplus V)$ and $U \oplus W = \mathbb{k} \cdot u \oplus (u^\perp \oplus W)$ with $\mathbb{k} \cdot u$ in the role of U . We get an isometric isomorphism between $u^\perp \oplus V$ and $u^\perp \oplus W$. Now apply the inductive hypothesis with u^\perp in the role of U to get the required isometry between V and W . \square

Corollary 17.2 *Let V be a space with a nonsingular symmetric bilinear form. Then in the orthogonal decomposition $V = H_{2k} \oplus U$ from Theorem 17.1 on p. 426, the hyperbolic space H_{2k} and anisotropic space U are determined by V uniquely up to isometry. In other words, given two such orthogonal decompositions*

$$V = H_{2k} \oplus U = H_{2m} \oplus W,$$

¹⁷The first orthogonal complement is taken in $U \oplus V$, the second in $U \oplus W$.

the anisotropic spaces U, W are isometrically isomorphic and the hyperbolic spaces have equal dimensions $2k = 2m$.

Proof Let $m \geq k$, that is, $H_{2m} = H_{2k} \oplus H_{2(m-k)}$. Since there is an identical isometry

$$\text{Id}_V : H_{2k} \oplus U \simeq H_{2k} \oplus H_{2(m-k)} \oplus W,$$

by Lemma 17.2 there exists an isometry $U \simeq H_{2(m-k)} \oplus W$. It forces $H_{2(m-k)} = 0$, because there are no isotropic vectors in U . Thus, $k = m$, and U is isometrically isomorphic to W . \square

Corollary 17.3 *Let V be a space with a nonsingular quadratic form q and let $U, W \subset V$ be some subspaces such that both restrictions $q|_U, q|_W$ are nonsingular. Then an isometry $\varphi : U \simeq W$, if such exists, can be extended (in many ways) to an isometric automorphism of V coinciding with φ on U .*

Proof It is enough to show that there exists some isometric isomorphism

$$\psi : U^\perp \simeq W^\perp.$$

Then $\varphi \oplus \psi : U \oplus U^\perp \simeq W \oplus W^\perp$, $(u, u') \mapsto (\varphi(u'), \psi(u'))$ is a required automorphism of V . By our assumptions the maps

$$\begin{aligned} \eta : U \oplus U^\perp &\rightarrow V, & (u, u') &\mapsto u + u', \\ \zeta : U \oplus W^\perp &\rightarrow V, & (u, w') &\mapsto \varphi(u) + w', \end{aligned}$$

both are isometric isomorphisms. The composition

$$\zeta^{-1} \eta : U \oplus U^\perp \simeq U \oplus W^\perp$$

is an isometric isomorphism as well. By Witt's lemma, U^\perp and W^\perp are isometrically isomorphic. \square

Corollary 17.4 *For each integer k in the range $1 \leq k \leq \dim V/2$, the orthogonal group of every nonsingular quadratic form on V acts transitively on k -dimensional isotropic subspaces and on $2k$ -dimensional hyperbolic subspaces in V .*

Proof The claim about hyperbolic subspaces follows from Corollary 17.3. It implies the claim about isotropic subspaces by Proposition 17.1. \square

17.3 Quadratic Forms over Real and Simple Finite Fields

In this section we enumerate all quadratic forms over \mathbb{R} and \mathbb{F}_p up to isometry.

17.3.1 Quadratic Forms over $\mathbb{F}_p = \mathbb{Z}/(p)$

Let $p > 2$ be prime number. Write $\varepsilon \in \mathbb{F}_p \setminus \mathbb{F}_p^2$ for a nonsquare, fixed once and for all. We know from Sect. 3.6.3 on p. 65 that the nonzero squares in \mathbb{F}_p form a subgroup of index 2 in the multiplicative group \mathbb{F}_p^* . This means that every nonzero element of \mathbb{F}_p is equivalent either to 1 or to ε modulo multiplication by nonzero squares. In particular, for every anisotropic vector v , there exists $\lambda \in \mathbb{F}_p^*$ such that $q(\lambda v) = \lambda^2 q(v)$ equals either 1 or ε .

Lemma 17.3 *For every $a, b \in \mathbb{F}_p^*$ and $c \in \mathbb{F}_p$, the equation $ax_1^2 + bx_2^2 = c$ is solvable in $x_1, x_2 \in \mathbb{F}_p$.*

Proof As x_1, x_2 run independently through \mathbb{F}_p , both quantities ax_1^2 and $c - bx_2^2$ take $(p + 1)/2$ different values in \mathbb{F}_p . Since $|\mathbb{F}_p| = p$, these two sets of values have at least one common element $ax_1^2 = c - bx_2^2$. \square

Proposition 17.2 *Every quadratic form q of rank r over \mathbb{F}_p , $p > 2$, is equivalent to $x_1^2 + \cdots + x_{r-1}^2 + x_r^2$ if $\det q_{\text{red}} \in \mathbb{F}_p^2$, and is equivalent to $x_1^2 + \cdots + x_{r-1}^2 + \varepsilon x_r^2$ if $\det q_{\text{red}} \notin \mathbb{F}_p^2$, where q_{red} is the reduced form¹⁸ on $V/\ker q$.*

Proof By Lagrange's theorem, Theorem 16.4 on p. 409,

$$q(x) = \alpha_1 x_1^2 + \alpha_2 x_2^2 + \cdots + \alpha_r x_r^2$$

in appropriate coordinates. It is enough to show that every linear combination of two squares $\alpha_i x_i^2 + \alpha_j x_j^2$ can be rewritten either as $x_1^2 + x_2^2$ or as $x_1^2 + \varepsilon x_2^2$. This can be done by means of Lemma 17.3. Write U for the linear span of vectors e_i, e_j . By Lemma 17.3, the map $q|_U : U \rightarrow \mathbb{k}$ is surjective. Hence, there exists $u \in U$ with $q(u) = 1$. The restriction of q to the 1-dimensional orthogonal to u in U is nonsingular, because both $q|_U$ and $q|_{\mathbb{F}_p \cdot u}$ are nonsingular. Therefore, the orthogonal to u in U is anisotropic and contains a vector w with $q(w)$ equal to either 1 or ε . \square

Proposition 17.3 *Up to isometry, there are exactly three anisotropic forms over \mathbb{F}_p with $p > 2$, namely $x_1^2, \varepsilon x_1^2$, and either $x_1^2 + x_2^2$, for $p \equiv -1 \pmod{4}$, or $x_1^2 + \varepsilon x_2^2$, for $p \equiv 1 \pmod{4}$.*

Proof By Lemma 17.3, every form $ax_1^2 + bx_2^2 + cx_3^2 + \cdots$ of rank ≥ 3 vanishes on a nonzero vector $(\alpha_1, \alpha_2, 1, 0, \dots)$ such that $a\alpha_1^2 + b\alpha_2^2 = -c$. Therefore, anisotropic forms over \mathbb{F}_p may exist only in dimensions 1 and 2. Both 1-dimensional nonzero forms $x_1^2, \varepsilon x_1^2$ certainly are anisotropic. The nondegenerate 2-dimensional forms up to isometry are exhausted by $q_1 = x_1^2 + x_2^2$ and $q_2 = x_1^2 + \varepsilon x_2^2$. We know from

¹⁸See Exercise 17.2 on p. 423.

Example 17.1 on p. 424 that q_1 has an isotropic vector if and only if $-\det q_1 = -1$ is a square in \mathbb{F}_p . By Sect. 3.6.3 on p. 65, this happens exactly for $p \equiv 1 \pmod{4}$. Since $\det q_2 = \varepsilon \det q_1$, the second form is anisotropic if and only if the first is not. \square

17.3.2 Real Quadratic Forms

By Theorem 16.4, every quadratic form q with real coefficients can be written in coordinates¹⁹ as

$$q(x) = x_1^2 + x_2^2 + \cdots + x_p^2 - x_{p+1}^2 - x_{p+2}^2 - \cdots - x_{p+m}^2. \quad (17.9)$$

The numbers p and m in (17.9) are called the *positive* and *negative inertia indices* of q , the ordered pair (p, m) is called the *signature* of q , the difference $p - m$ is called just the *index* of q . Let us verify that all these quantities do not depend on the choice of coordinates, where q looks like (17.9).

Of course, $p + m = \operatorname{rk} q$ does not depend on the basis. Replacing V by $V/\ker q$, we may assume that q is not singular. Then V splits into an orthogonal direct sum of hyperbolic and anisotropic subspaces, both unique up to isometry. Such a decomposition is read off easily from the presentation (17.9). Namely, each pair of orthogonal coordinates with signature $(1, 1)$ produces a hyperbolic plane: $x_1^2 - x_2^2 = (x_1 + x_2)(x_1 - x_2) = 2y_1y_2$, where $y_{1,2} = (x_1 \pm x_2)/\sqrt{2}$. The remaining sum of either purely positive or purely negative squares is anisotropic. Therefore, the dimension of the hyperbolic component of q is $2 \min(p, m)$, and the dimension of the anisotropic component is $|p - m|$. The sign of the difference $p - m$ shows which of the two inequivalent anisotropic forms α appears in q : *positive*,²⁰ which gives $\alpha(v) > 0$ for all $v \neq 0$, or *negative*, which gives $\alpha(v) < 0$ for all $v \neq 0$. Since p, q are uniquely recovered from $p + m$ and $p - m$, we get the following proposition.

Proposition 17.4 *Two real quadratic forms are equivalent if and only if they have equal ranks and indices. For each $n \in \mathbb{N}$, there are exactly two anisotropic forms of rank n . They have indices $\pm n$.* \square

Exercise 17.8 Show that $p = \max \dim U$ over all $U \subset V$ such that $q|_U$ is positive anisotropic, and $q = \max \dim U$ over all $U \subset V$ such that $q|_U$ is negative anisotropic.

¹⁹Choose any orthogonal basis e_1, e_2, \dots, e_n for q and divide all e_i such that $q(e_i) \neq 0$ by $\sqrt{|q(e_i)|}$.

²⁰That is, *Euclidean*.

17.3.3 How to Find the Signature of a Real Form

Fix a basis in V and write V_k for the linear span of the first k basis vectors e_1, e_2, \dots, e_k . Let Δ_k be the Gram determinant of the restriction $q|_{V_k}$, or equivalently, the principal upper left $k \times k$ minor²¹ of the Gram matrix of q . It vanishes if and only if $q|_{V_k}$ is singular. Otherwise, the sign of Δ_k equals $(-1)^{m_k}$, where m_k is the negative inertia index of $q|_{V_k}$. Reading the sequence $\Delta_1, \Delta_2, \dots, \Delta_{\dim V}$ from left to right, we can track signature changes under passing from V_i to V_{i+1} or detect the appearance of isotropic vectors. In many cases, such an analysis allows us to determine the total signature of q .

For example, let $\Delta_1 < 0$, $\Delta_2 = 0$, $\Delta_3 > 0$, $\Delta_4 = 0$, $\Delta_5 = 0$, $\Delta_6 < 0$. Since $q|_{V_2}$ is singular, V_2 is the direct orthogonal sum of the negative anisotropic line $\mathbb{R}e_1$ and an isotropic line. Since V_3 is not singular, the orthogonal to e_1 within V_3 is nonsingular and contains an isotropic vector. Hence it must be a hyperbolic plane, i.e., $V_3 = \mathbb{R}e_1 \oplus H_2$. Note that this *forces* Δ_3 to be of opposite sign with respect to Δ_1 , and this agrees with our data.

Exercise 17.9 Let $\Delta_{i-1} \neq 0$, $\Delta_i = 0$, and $\Delta_{i+1} \neq 0$ in a sequence of principal upper left minors. Show that $\Delta_{i-1}\Delta_{i+1} < 0$ and $V_{i+1} = V_{i-1} \oplus H_2$.

Thus, V_3 has signature $(1, 2)$. The same arguments as above show that V_3^\perp is nondegenerate and contains an isotropic vector. Therefore, the signature of V_3^\perp is either $(2, 1)$ or $(1, 2)$. Since Δ_3 and Δ_6 are of opposite signs, we conclude that the first case occurs. Thus, the total signature of q is $(1, 2) + (2, 1) = (3, 3)$. An example of such a form is provided by the Gramian

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

If all minors Δ_k are nonzero, then all restrictions $q|_{V_k}$ are nonsingular, and the signs of Δ_{i+1} and Δ_i are different if and only if $m_{i+1} = m_i + 1$. Therefore, the negative inertia index m equals the number of sign inversions in the sequence $1, \Delta_1, \Delta_2, \dots, \Delta_{\dim V}$, in this case. This remark is known as *Sylvester's law of inertia*.

²¹That is, the determinant of the submatrix formed by the topmost k rows and leftmost k columns.

17.4 Projective Quadrics

17.4.1 Geometric Properties of Projective Quadrics

A projective hypersurface²² $Q = Z(q) = \{v \in \mathbb{P}(V) \mid q(v) = 0\}$ formed by isotropic vectors of a nonzero quadratic form $q \in S^2V^*$ is called a *projective quadric*. Quadrics in \mathbb{P}_2 are called *conics*, and quadrics in \mathbb{P}_3 are called *quadratic surfaces*. Since proportional forms define the same quadric, projective quadrics correspond to the points of the projective space of quadrics²³ $\mathbb{P}(S^2V^*)$. Two projective quadrics in $\mathbb{P}(V)$ are called *projectively equivalent*²⁴ if there exists a linear projective automorphism $\mathbb{P}(V) \xrightarrow{\sim} \mathbb{P}(V)$ sending one of them to the other.

As above, we write $\tilde{q} : V \times V \rightarrow \mathbb{k}$ for the polarization²⁵ of a quadratic form $q \in S^2V^*$, and $\hat{q} : V \rightarrow V^*$ for the correlation map,²⁶ which takes a vector $v \in V$ to the covector $u \mapsto \tilde{q}(u, v)$. The projectivization of the kernel of the correlation map,

$$\text{Sing } Q \stackrel{\text{def}}{=} \mathbb{P}(\ker \hat{q}) = \mathbb{P}\{w \in V \mid \forall u \in V \tilde{q}(u, w) = 0\}, \quad (17.10)$$

is called the *singular locus*²⁷ of the quadric $Q = Z(q)$. A quadric Q is called *smooth*²⁸ if $\text{Sing } Q = \emptyset$. Otherwise, Q is called *singular* or *degenerate*. Note that $\text{Sing } Q \subset Q$ is a projective subspace lying on Q . In particular, every singular quadric is nonempty. All points $a \in \text{Sing } Q$ are called *singular points* of Q ; all the other points $a \in Q \setminus \text{Sing } Q$ are called *smooth*.

Example 17.3 (Quadrics on the Projective Line, the Geometric Version of Example 17.1) In Example 17.1 on p. 424, we have seen that on \mathbb{P}_1 there exists a unique, up to isomorphism, singular quadric. It may be given by the equation $x_0^2 = 0$ and is called a *double point*. Smooth quadrics $Q = Z(q)$ are of two types. If $-\det q$ is a square, then Q may be given by the equation $x_0x_1 = 0$, which constitutes a pair of distinct points. If $-\det q$ is not a square, then $Q = \emptyset$. The latter never happens over an algebraically closed field.

Corollary 17.5 *The positional relationships between a line ℓ and a quadric Q in projective space are exhausted by the following alternative variants: either $\ell \subset Q$, or $\ell \cap Q$ is a double point, or $\ell \cap Q$ is a pair of distinct points, or $\ell \cap Q = \emptyset$. The last case is impossible over an algebraically closed field. \square*

²²See Sect. 11.3 on p. 263.

²³See Sect. 11.3.3 on p. 265.

²⁴Or *isomorphic*.

²⁵See Sect. 17.1 on p. 421.

²⁶See Sect. 16.1 on p. 387.

²⁷Or *vertex subspace*.

²⁸Other names: *nonsingular* and *nondegenerate*.

Definition 17.1 (Tangent Lines and Tangent Space) Let Q be a projective quadric and $a \in Q$ a point. A line $\ell \ni a$ is called *tangent* to Q at a if either $\ell \subset Q$ or $\ell \cap Q$ is a double point at a . The union of all lines tangent to a quadric Q at a point $a \in Q$ is called the *tangent space* of Q at a and is denoted by $T_a Q$.

Lemma 17.4 A line (ab) is tangent to a quadric $Q = Z(q)$ at a point $a \in Q$ if and only if $\tilde{q}(a, b) = 0$.

Proof Write $U \subset V$ for the linear span of the vectors $a, b \in V$. The restriction $q|_U$ is either zero or singular if and only if its Gramian $G = \begin{pmatrix} 0 & \tilde{q}(a, b) \\ \tilde{q}(a, b) & \tilde{q}(b, b) \end{pmatrix}$ has $\det G = \tilde{q}(a, b)^2 = 0$. \square

Corollary 17.6 If a point $a \in Q = Z(q) \subset \mathbb{P}(V)$ is smooth, then

$$T_a Q = \{x \in \mathbb{P}_n \mid \tilde{q}(a, x) = 0\}$$

is a hyperplane. If $a \in \text{Sing } Q$, then $T_a Q = \mathbb{P}(V)$, i.e., every line passing through a either lies on Q or does not intersect Q anywhere outside a .

Proof The linear equation $\tilde{q}(a, x) = 0$ either defines a hyperplane or is satisfied identically in x . The latter means that $a \in \ker q$. \square

Remark 17.1 By [Exercise 17.1](#) on p. 422, the linear equation $\tilde{q}(a, x) = 0$, which determines the tangent space of the quadric $Z(q)$ at the point $a \in Z(q)$, can be written as $\sum \frac{\partial q}{\partial x_i}(a) \cdot x_i = 0$. In particular, a point a is singular if and only if all partial derivatives $\partial q / \partial x_i$ vanish at a .

Corollary 17.7 (Apparent Contour) The apparent contour of a quadric $Q = Z(q)$ viewed from a point²⁹ $b \notin Q$ is cut out of Q by the hyperplane

$$b^\perp = \text{Ann } \hat{q}(b) = \{x \mid \tilde{q}(b, x) = 0\}.$$

Proof If $b \notin Q$, then $\tilde{q}(b, b) = q(b) \neq 0$. Therefore, the linear equation $\tilde{q}(b, x) = 0$ is nontrivial and defines a hyperplane. \square

Proposition 17.5 If a quadric $Q \subset \mathbb{P}_n$ has a smooth point $a \in Q$, then Q is not contained in a hyperplane.

Proof For $n = 1$, this follows from [Example 17.3](#). Consider $n \geq 2$. If Q lies within a hyperplane H , then every line $\ell \not\subset H$ passing through a intersects Q only in a and therefore is tangent to Q at a . Hence, $\mathbb{P}_n = H \cup T_p Q$. This contradicts [Exercise 17.10](#) below. \square

²⁹That is, the locus of all points $a \in Q$ such that the line (ba) is tangent to Q at a .

Exercise 17.10 Show that projective space over a field of characteristic $\neq 2$ is not a union of two hyperplanes.

Theorem 17.3 Let $Q \subset \mathbb{P}_n$ be an arbitrary quadric and $L \subset \mathbb{P}_n$ a projective subspace complementary³⁰ to $\text{Sing } Q$. Then $Q' = L \cap Q$ is a smooth quadric in L , and Q is the linear join³¹ of Q' and $\text{Sing } Q$.

Proof The smoothness of Q' follows from Proposition 16.6 on p. 409. Every line intersecting $\text{Sing } Q$ either belongs to $\text{Sing } Q$ or can be written as (ab) for some $a \in \text{Sing } Q$ and $b \in L$. By Corollary 17.6, the line (ab) either lies on Q , in which case $b \in Q'$, or does not intersect Q anywhere except at a . \square

Example 17.4 (Singular Conics) Let $C \subset \mathbb{P}_2$ be a singular conic. If $\text{Sing } C = s$ is a point, then by Theorem 17.3, C is formed by lines joining s with the points of a nonsingular quadric $Q' \subset \ell$ living within some line $\ell \not\ni s$. If $Q' \neq \emptyset$, then C is a pair of crossing lines. If $Q' = \emptyset$, then $C = s$, and this never happens over an algebraically closed field. If $\text{Sing } C$ is a line, then C is exhausted by this line, because the nonsingular quadric within the complementary point \mathbb{P}_0 is empty. Such a C is called a *double line*, because its equation is the perfect square of a linear form.

Exercise 17.11 Show that every rank-1 quadratic form is the perfect square of a linear form and give a geometric classification of singular quadratic surfaces in \mathbb{P}_3 similar to Example 17.4.

Example 17.5 (Veronese Conic) Consider $\mathbb{P}_1 = \mathbb{P}(U)$ and write $S^2\mathbb{P}_1$ for the set of unordered pairs of points $\{a, b\} \subset \mathbb{P}_1$, where $a = b$ is allowed as well. Over an algebraically closed field, there is canonical bijection

$$S^2\mathbb{P}_1 \xrightarrow{\sim} \mathbb{P}_2 = \mathbb{P}(S^2U^*),$$

which takes $\{a, b\} \subset \mathbb{P}(U)$ to the quadratic form $q_{a,b}(x) = \det(x, a) \cdot \det(x, b)$, the equation for $Q = \{a, b\}$ in some homogeneous coordinates $x = (x_0 : x_1)$ on \mathbb{P}_1 , where

$$\det(x, p) \stackrel{\text{def}}{=} \det \begin{pmatrix} x_0 & p_0 \\ x_1 & p_1 \end{pmatrix} = p_1x_0 - p_0x_1 \text{ for } p = (p_0 : p_1) \in \mathbb{P}_1.$$

In the basis $x_0^2, 2x_0x_1, x_1^2$ for S^2U^* , where the quadratic form $\vartheta_0x_0^2 + 2\vartheta_1x_0x_1 + \vartheta_2x_1^2$ has coordinates $(\vartheta_0 : \vartheta_1 : \vartheta_2)$, the form $q_{a,b}(x)$ corresponding to the points $a = (\alpha_0 : \alpha_1)$ and $b = (\beta_0 : \beta_1)$ has coordinates $(-2\alpha_1\beta_1 : \alpha_0\beta_1 + \alpha_1\beta_0 : -2\alpha_0\beta_0)$.

³⁰See Sect. 11.4 on p. 268.

³¹That is, the union of all lines (ab) , where $a \in Q', b \in \text{Sing } Q$.

Pairs of coinciding points $\{a, a\}$ are mapped bijectively onto the *Veronese conic* $C \subset S^2U^*$, which consists of rank-one quadratics³² and is described by the equation

$$\det \begin{pmatrix} \vartheta_0 & \vartheta_1 \\ \vartheta_1 & \vartheta_2 \end{pmatrix} = \vartheta_0\vartheta_2 - \vartheta_1^2 = 0. \quad (17.11)$$

For fixed a and varying b , the quadratic forms $q_{a,b}$ form a line in S^2U^* meeting C in exactly one point $q_{a,a}$. Identifying the points of \mathbb{P}_2 with pairs $\{a, b\} \subset \mathbb{P}_1$ and Veronese's conic with double points $\{a, a\}$, we can say that the line tangent to C at $\{a, a\}$ consists of all $\{a, b\}$, $b \in \mathbb{P}_1$.

Exercise 17.12 Show geometrically that each nontrivial involution³³ of \mathbb{P}_1 has exactly two distinct fixed points and construct a bijection between involutions and points of $S^2\mathbb{P}_1 \setminus C$.

Proposition 17.6 *Let $C \subset \mathbb{P}_2$ be a smooth conic and $D \subset \mathbb{P}_2$ a curve of degree d . Then either $C \subset D$ or C intersects D in at most $2d$ points.*

Proof Let $D = Z(f)$ and $C = Z(q)$. If $C = \emptyset$, there is nothing to prove. If there is some $a \in C$, choose any line $\ell \not\ni a$ and consider the projection $\pi_a : C \rightarrow \ell$ from a onto ℓ . It is bijective, because each line $(ab) \neq T_a C$, $b \in \ell$, intersects C in exactly one point $c \neq a$, namely, in

$$c(b) = q(b) \cdot a + \tilde{q}(a, b) \cdot b.$$

Exercise 17.13 Verify this and check that for $b = T_a C \cap \ell$, we get $c = a$.

The inverse map $\varphi : \ell \xrightarrow{\sim} C$, $b \mapsto c(b) = (ab) \cap C$, provides C with a homogeneous parametrization quadratic in b . Substituting $x = c(b)$ in the equation for D , we get $f(q(b) \cdot a + \tilde{q}(a, b) \cdot b) = 0$, which is either the trivial identity $0 = 0$ or a nontrivial homogeneous equation of degree $2d$ in b . In the first case, $C \subset D$. In the second case, there are at most $2d$ roots. \square

Exercise 17.14 Let \mathbb{k} be a field with $\text{char } \mathbb{k} \neq 2$. Show that:

- (a) Every five points in \mathbb{P}_2 lie on a conic.
- (b) If no four of the points are collinear, then such a conic is unique.
- (c) If no three of the points are collinear, then the conic is smooth.

³²That is, perfect squares; see [Exercise 17.11](#).

³³That is, a nonidentical linear projective automorphism $\sigma : \mathbb{P}_1 \xrightarrow{\sim} \mathbb{P}_1$ such that $\sigma^2 = \text{Id}_{\mathbb{P}_1}$.

Example 17.6 (Segre Quadric) Fix a 2-dimensional vector space U , put $W = \text{End}(U)$, and consider $\mathbb{P}_3 = \mathbb{P}(W)$. Write

$$Q_s \stackrel{\text{def}}{=} \{F : \in \text{End}(U) \mid \det F = 0\} = \left\{ \begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix} \mid x_0x_3 - x_1x_2 = 0 \right\} \subset \mathbb{P}_3 \quad (17.12)$$

for the quadric formed by endomorphisms of rank 1 considered up to proportionality. This quadric is called *Segre's quadric*. Every rank-1 operator $F : U \rightarrow U$ has a 1-dimensional image spanned by some vector $v \in U$, uniquely determined by F up to proportionality. Then the value of F on every $u \in U$ equals $F(u) = \xi(u) \cdot v$, where $\xi \in U^*$ is a linear form such that $\text{Ann } \xi = \ker F$. Therefore, ξ is also uniquely determined by F up to proportionality. Conversely, for every nonzero $v \in U$, $\xi \in U^*$, the operator

$$\xi \otimes v : U \rightarrow U, \quad u \mapsto \xi(u)v,$$

has rank 1. Therefore, there is a well-defined injective map

$$s : \mathbb{P}(U^*) \times \mathbb{P}(U) \hookrightarrow \mathbb{P} \text{End}(U), \quad (\xi, v) \mapsto \xi \otimes v, \quad (17.13)$$

whose image is precisely the Segre quadric (17.12). The map (17.13) is called *Segre's embedding*.

Every 2×2 matrix of rank 1 has proportional rows and proportional columns. If we fix either of the ratios:

$$\begin{aligned} ([\text{row } 1] : [\text{row } 2]) &= (t_0 : t_1), \\ ([\text{column } 1] : [\text{column } 2]) &= (\xi_0 : \xi_1), \end{aligned}$$

then we get a 2-dimensional vector subspace in W formed by the rank-1 matrices with the fixed ratio. After projectivization, it is a line on the Segre quadric. We conclude that Segre's quadric is ruled by two families of lines, the images of “coordinate lines” $\mathbb{P}_1^\times \times v$ and $\xi \times \mathbb{P}_1$ on $\mathbb{P}_1^\times \times \mathbb{P}_1$ under the Segre embedding (17.13). Indeed, the operator $\xi \otimes v$ coming from $\xi = (\xi_0 : \xi_1) \in U^*$ and $v = (t_0 : t_1) \in U$ has matrix

$$\begin{pmatrix} t_0 \\ t_1 \end{pmatrix} \cdot (\xi_0 \ \xi_1) = \begin{pmatrix} \xi_0 t_0 & \xi_1 t_0 \\ \xi_0 t_1 & \xi_1 t_1 \end{pmatrix} \quad (17.14)$$

with prescribed ratios between rows and columns.

Since the Segre embedding establishes a bijection between $\mathbb{P}_1^\times \times \mathbb{P}_1$ and Q_s , the incidence relations among the coordinate lines in $\mathbb{P}_1^\times \times \mathbb{P}_1$ are the same as among their images in Q_s . This means that within each ruling family, all the lines are mutually skew,³⁴ every two lines from different ruling families are intersecting, and

³⁴That is, nonintersecting (or complementary).

each point on the Segre quadric is an intersection point of exactly two lines from different families. Moreover, all lines $\ell \subset Q_s$ are exhausted by these two ruling families, because every line $\ell \subset Q_s$ belongs to $Q_s \cap T_a Q_s$ for some $a \in Q_s$, and the conic $T_a Q_s \cap Q_s$ is exhausted by two ruling lines crossing at a .

Exercise 17.15 Show that (a) every nine points, (b) every three lines in \mathbb{P}_3 lie on some quadric. Prove that the quadric passing through three mutually skew lines is unique and is isomorphic to the Segre quadric.

17.4.2 Smooth Quadrics

For every nonsingular quadratic form $q \in S^2 V^*$, the orthogonal operators $F \in O_q(V)$ produce linear projective automorphisms $\mathbb{P}(V) \simeq \mathbb{P}(V)$ sending the quadric $Q = Z(q)$ to itself. They are called the *automorphisms* of the smooth projective quadric Q . By Corollary 17.4, the automorphisms of Q act transitively on the points of Q and on the projective subspaces $L \subset Q$ of any given dimension. In particular, $\max \dim L$ taken over all subspaces $L \subset Q$ passing through a given point $a \in Q$ is the same for all $a \in Q$. This maximal dimension is called the *planarity* of Q and denoted by $m(Q)$. Smooth quadrics of different planarities are clearly not isomorphic.

By Corollary 17.2 on p. 430, every smooth quadric $Q = Z(q) \subset \mathbb{P}_n = \mathbb{P}(V)$ can be given in appropriate coordinates by the equation

$$x_0 x_1 + x_2 x_3 + \cdots + x_{2m} x_{2m+1} + \alpha(x_{2m+2}, \dots, x_n) = 0, \quad (17.15)$$

where $\alpha(x) \neq 0$ for all $x \neq 0$, and $m + 1 \in \mathbb{N}$ is equal to the dimension of the maximal isotropic subspace of q in V . We conclude that the quadric (17.15) has planarity m . Therefore, for different m , the equations (17.15) constitute projectively inequivalent quadrics. Note that the planarity $m = -1$ is allowed as well and means that $Z(q) = Z(\alpha) = \emptyset$.

Example 17.7 (Smooth Quadrics over an Algebraically Closed Field) Over an algebraically closed field, the only anisotropic form is the 1-dimensional form x^2 . Hence, for each $n \in \mathbb{N}$, there exists exactly one smooth n -dimensional quadric $Q_n \subset \mathbb{P}_{n+1}$ up to isomorphism. For even $n = 2m$, it can be defined by the equation

$$x_0 x_1 + x_2 x_3 + \cdots + x_{2m} x_{2m+1} = 0; \quad (17.16)$$

for odd $n = 2m + 1$ it can be defined by the equation

$$x_0 x_1 + x_2 x_3 + \cdots + x_{2m} x_{2m+1} = x_{2m+2}^2. \quad (17.17)$$

The planarity of both quadrics (17.16), (17.17) is m , that is, some m -dimensional projective subspace $L \subset Q_n$ can be drawn through each point $a \in Q_n$, and there are no $(m + 1)$ -dimensional subspaces lying on Q_n .

Example 17.8 (Smooth Real Quadrics) For $\mathbb{k} = \mathbb{R}$, in each dimension $k \in \mathbb{N}$ there exists a unique, up to a sign, anisotropic form

$$\alpha_k(x_1, x_2, \dots, x_k) = x_1^2 + x_2^2 + \dots + x_k^2.$$

Hence, every smooth n -dimensional quadric in $\mathbb{P}_{n+1} = \mathbb{P}(\mathbb{R}^{n+2})$ can be represented by the equation

$$x_0x_1 + x_2x_3 + \dots + x_{2m}x_{2m+1} = x_{2m+2}^2 + x_{2m+3}^2 + \dots + x_{n+1}^2, \quad (17.18)$$

where $-1 \leq m \leq n/2$. We denote this quadric by $Q_{n,m}$ and call it an n -dimensional m -planar smooth real quadric. The quadratic form (17.18) has signature

$$(n + 2 - m, m).$$

and index $n + 2 - 2m$. Any one of these quantities characterizes a smooth n -dimensional real quadric uniquely up to isomorphism. For $m \geq 0$, all quadrics $Q_{n,m}$ are projectively inequivalent. All (-1) -planar quadrics $Q_{n,-1}$ with anisotropic equations $x_0^2 + x_1^2 + \dots + x_n^2 = 0$ are empty.

In orthogonal coordinates, the quadric $Q_{n,m}$ is given by the equation

$$t_0^2 + t_1^2 + \dots + t_m^2 = t_{m+1}^2 + t_{m+2}^2 + \dots + t_{n+1}^2.$$

The hyperbolic coordinates x_v are expressed in terms of orthogonal coordinates t_v as $x_{2i} = t_{m+i} + t_i$, $x_{2i+1} = t_{m+i} - t_i$ for $0 \leq i \leq m$ and $x_j = t_j$ for $2m + 2 \leq j \leq n + 2$.

The 0-planar quadric $t_0^2 = t_1^2 + t_2^2 + \dots + t_n^2$, is called *elliptic*. All quadrics of higher planarities are traditionally called *hyperbolic*, although this is not quite correct, because the equation of such a quadric is a purely hyperbolic form only for $n = 2m$.

Proposition 17.7 *For every smooth quadric Q and hyperplane Π , the intersection $\Pi \cap Q \subset \Pi$ either is a smooth quadric in Π or has exactly one singular point p . In the latter case, $\Pi = T_p Q$, and the quadric $\Pi \cap Q$ is a cone with vertex p over the smooth quadric $Q' = \Pi' \cap Q$ cut out of Q by any codimension-1 subspace $\Pi' \subset T_p Q$ complementary to p . Furthermore, for the planarity, we have $m(Q') = m(Q) - 1$.*

Proof Let $Q = Z(q) \subset \mathbb{P}(V)$ and $\Pi = \mathbb{P}(W)$. Then

$$\begin{aligned} \dim \ker(\hat{q}|_W) &= \dim \left(W \cap \hat{q}^{-1}(\text{Ann } W) \right) \leq \dim \hat{q}^{-1}(\text{Ann } W) \\ &= \dim \text{Ann } W = \dim V - \dim W = 1. \end{aligned}$$

Let $\dim \ker(\hat{q}|_W) = 1$ and suppose that p spans the kernel. Since $p \in Q \cap \Pi$ and $\text{Ann}(\hat{q}(p)) = W$, we conclude that $T_p Q = \Pi$. Conversely, if $\Pi = T_p Q = \mathbb{P}(\text{Ann} \hat{q}(p))$ for some point $p \in Q$, then $p \in \text{Ann} \hat{q}(p)$ lies in the kernel of the restriction of \hat{q} to $\text{Ann} \hat{q}$, and it spans this kernel, because it is 1-dimensional. This proves the first two statements of the proposition. By Theorem 17.3 on p. 437, the restriction of q to any codimension-1 subspace $\Pi' = \mathbb{P}(U) \subset T_p Q$ complementary to p is nonsingular. Therefore, $V = U \oplus U^\perp$, where $\dim U^\perp = 2$ and the restriction $q|_{U^\perp}$ is nonsingular too. Since $p \in U^\perp$ is isotropic for $q|_{U^\perp}$, the subspace $U^\perp \subset V$ is a hyperbolic plane. Hence, the dimension of the hyperbolic component of the form $q|_U$ is two less than the dimension of the hyperbolic component of q . Since $Q' = Z(q|_U)$, the last statement of the proposition holds. \square

Corollary 17.8 *Let $Q \subset \mathbb{P}_n$ be a smooth quadric of planarity m and $p \in Q$ any point. Write $Q' = Q \cap \mathbb{P}_{n-2}$ for the quadric of planarity $(m-1)$ cut out of Q by any codimension-1 subspace $\mathbb{P}_{n-2} \subset T_p Q = \mathbb{P}_{n-1}$ complementary to p . Then the m -dimensional subspaces $L \subset Q$ passing through p are in bijection with the set of all $(m-1)$ -dimensional subspaces $L' \subset Q'$.* \square

Example 17.9 (Subspaces on Smooth Quadrics over an Algebraically Closed Field) If \mathbb{k} is algebraically closed, then the smooth quadrics $Q_0 \subset \mathbb{P}_1$ and $Q_1 \subset \mathbb{P}_2$ both are 0-planar. The next two quadrics $Q_2 \subset \mathbb{P}_3$ and $Q_3 \subset \mathbb{P}_4$ are 1-planar. For every $p \in Q_2$, there are exactly two lines $\ell \subset Q_2$ passing through p . They join p with two points of some smooth quadric $Q_0 \subset \mathbb{P}_1 \subset T_p Q_2 \setminus \{p\}$. Note that this agrees with Example 17.6. The lines $\ell \subset Q_3$ passing through a given point $p \in Q_3$ join p with the points of some smooth conic $Q_1 \subset \mathbb{P}_2 \subset T_p Q_3 \setminus \{p\}$ and form a cone with its vertex at p . The next, 4-dimensional, smooth quadric $Q_4 \subset \mathbb{P}_5$, is 2-planar. Each plane $\pi \subset Q_4$ passing through a given point $p \in Q_4$ is spanned by p and some line on Segre's quadric $Q_2 \subset \mathbb{P}_3 \subset T_p Q_4 \setminus \{p\}$. Thus, these planes split into two pencils corresponding to two line rulings of Q_2 .

Example 17.10 (Subspaces on Real Smooth Quadrics) For $\mathbb{k} = \mathbb{R}$ and every dimension n , the smooth elliptic quadric $Q_{n,0}$ is 0-planar and contains no lines. Each point p of the 1-planar quadric $Q_{n,1}$ is a vertex of the cone ruled by the lines joining p with the points of some smooth $(n-2)$ -dimensional elliptic quadric $Q_{n-2,0} \subset \mathbb{P}_{n-1} \subset T_p Q_{n,1} \setminus \{p\}$. All these lines lie on $Q_{n,1}$, and there are no other lines on $Q_{n,1}$ passing through p . In particular, each point p on the real Segre's quadric $Q_{2,1} \subset \mathbb{P}_3$ is an intersection point of two lines passing through two points of the 0-dimensional elliptic quadric $Q_{0,0} \subset \mathbb{P}_1 \subset T_p Q_{2,1} \setminus \{p\}$.

17.4.3 Polarities

Recall that we write $\hat{q} : V \rightarrow V^*$ for the correlation map³⁵ associated with the nonsingular symmetric bilinear form \tilde{q} . It sends a vector $v \in V$ to the linear form $\hat{q}v : u \mapsto \tilde{q}(u, v)$ on V and produces a linear projective isomorphism $\bar{q} : \mathbb{P}(V) \rightarrow \mathbb{P}(V^*)$ called the *polar map* (or just the *polarity* for short) associated with the smooth quadric $Q = Z(q) \subset \mathbb{P}(V)$. If we interpret $\mathbb{P}(V^*)$ as the space of hyperplanes in $\mathbb{P}(V)$, then we can say that the polarity \bar{q} sends a point $a \in \mathbb{P}_n$ to the hyperplane $\Pi_a \subset \mathbb{P}_n$ described by the linear equation $\tilde{q}(x, a) = 0$ in x . The point a and the hyperplane Π_a are called the *pole* and *polar* of each other with respect to Q . If $a \notin Q$, then Π_a cuts the apparent contour³⁶ of Q viewed from a , i.e., $\Pi_a \cap Q = \{b \in Q \mid a \in T_b Q\}$. If $a \in Q$, then $\Pi_a = T_a Q$. Thus, the quadric Q is recovered from the polar map as the locus of all points lying on their own polars. Since the orthogonality condition $\tilde{q}(a, b) = 0$ is symmetric in a, b , the point a lies on the polar of the point b if and only if the point b lies on the polar of a . This claim is known as *polar duality*. Points a, b such that $\tilde{q}(a, b) = 0$ are called *conjugate* with respect to the quadric Q .

Proposition 17.8 *Let Q be a smooth quadric and $a, b \notin Q$ two different points such that the line $\ell = (ab)$ intersects Q in two different points c, d . Then a, b are conjugate with respect to Q if and only if the pair $\{a, b\}$ is harmonic³⁷ to the pair $\{c, d\}$ on the line ℓ .*

Proof Let $Q = Z(q)$ and write $x = (x_0 : x_1)$ for the homogeneous coordinates on ℓ in the basis $c, d \in \ell$. In these coordinates, the restriction of q onto ℓ is given, up to proportionality, by the quadratic form $q(x) = \det(x, c) \cdot \det(x, d)$.

Taking the polarization, we get a symmetric bilinear form in $x = (x_0 : x_1)$ and $y = (y_0 : y_1)$:

$$\tilde{q}(x, y) = \frac{1}{2} (\det(x, c) \cdot \det(y, d) + \det(y, c) \cdot \det(x, d)).$$

The orthogonality condition $\tilde{q}(a, b) = 0$ is equivalent to the relation

$$\det(a, c) \cdot \det(b, d) = -\det(b, c) \cdot \det(a, d),$$

which says that $[a, b, c, d] = -1$. □

Proposition 17.9 *Let $G \subset \mathbb{P}_n$ be a smooth quadric with Gramian Γ , and $Q \subset \mathbb{P}_n$ an arbitrary quadric with Gramian B in the same basis. Then the polar map $\mathbb{P}_n \rightarrow \mathbb{P}_n^\times$ provided by G sends Q to a quadric in \mathbb{P}_n^\times with Gramian $\Gamma^{-1}B\Gamma^{-1}$ in the dual basis.*

³⁵See Sect. 16.1 on p. 387.

³⁶See Corollary 17.7 on p. 436.

³⁷This means that the cross ratio satisfies $[a, b, c, d] = -1$ (see Sect. 11.6.3 on p. 274).

Proof In coordinates with respect to any dual bases in V and V^* , the correlation $\hat{g} : V \simeq V^*$ takes a vector with coordinate row x to the covector with coordinate row $y = x\Gamma$. If the vector x is constrained by the relation $x B x^t = 0$, then the substitution $x \leftarrow y\Gamma^{-1}$ shows that the covector $y = x\Gamma$ satisfies the relation $y\Gamma^{-1}B(\Gamma^{-1})^t y^t = y\Gamma^{-1}B\Gamma^{-1}y^t = 0$ (we have used that Γ is symmetric and invertible). Conversely, if $y\Gamma^{-1}B\Gamma^{-1}y^t = 0$, then for $x = y\Gamma^{-1}$, the relation $x B x^t = 0$ holds. \square

Corollary 17.9 *The tangent spaces of a smooth quadric $S \subset \mathbb{P}_n$ form a smooth quadric $S^\times \subset \mathbb{P}_n^\times$. The Gramians of S and S^\times in dual bases of \mathbb{P}_n and \mathbb{P}_n^\times are inverse to each other.*

Proof Apply Proposition 17.9 for $G = Q = S$. \square

Proposition 17.10 *Over an infinite field, two nonempty smooth quadrics coincide if and only if their equations are proportional.*

Proof Let $Z(q_1) = Z(q_2)$ in $\mathbb{P}(V)$. Then the two polarities $\bar{q}_1, \bar{q}_2 : \mathbb{P}(V) \simeq \mathbb{P}(V^*)$ coincide at all points of the quadrics.

Exercise 17.16 Check that over an infinite field, every nonempty smooth quadric in \mathbb{P}_n contains $n + 2$ points such that no $(n + 1)$ of them lie within a hyperplane.

It follows from Exercise 17.16 and Theorem 11.1 on p. 270 that the correlation maps $\hat{q}_1, \hat{q}_2 : V \simeq V^*$ are proportional. Therefore, the Gramians are proportional. \square

17.5 Affine Quadrics

17.5.1 Projective Enhancement of Affine Quadrics

Everywhere in this section we assume that the ground field \mathbb{k} is infinite and $\text{char } \mathbb{k} \neq 2$. Let V be a vector space and $f \in SV^*$ a polynomial of degree 2, not necessarily homogeneous. An affine hypersurface³⁸ $X = Z(f) = \{v \in V \mid f(v) = 0\} \subset \mathbb{A}(V)$ is called an *affine quadric*. Two affine quadrics $X_1, X_2 \subset \mathbb{A}(V)$ are called *affinely equivalent*³⁹ if there exists an affine automorphism $F : \mathbb{A}(V) \simeq \mathbb{A}(V)$ such that $F(X_1) = X_2$.

Every affine quadric $X = Z(f) \subset \mathbb{A}(V)$ admits a *projective enhancement* provided by the *projective closure* construction from Sect. 11.3.2 on p. 264. We put $W = \mathbb{k} \oplus V$, $e_0 = (1, 0) \in \mathbb{k} \oplus V$, and write $x_0 \in W^*$ for the unique basis vector in $\text{Ann } V$ such that $x_0(e_0) = 1$. We decompose the affine equation for X into homogeneous parts, $f = f_0 + f_1 + f_2$, where $f_0 \in \mathbb{k}, f_1 \in V^*, f_2 \in S^2 V^*$, and put

$$q = \bar{f} = f_0 \cdot x_0^2 + f_1 \cdot x_0 + f_2 \in S^2 W^*. \quad (17.19)$$

³⁸See Sect. 11.2.4 on p. 262.

³⁹Or *isomorphic*.

Then $q(e + v) = f(v)$ for all $v \in V$. The projective quadric $Q = Z(q) \subset \mathbb{P}(W)$ is called the *projective closure* of X , and the quadratic form $q \in S^2 W^*$ is called the *extended* quadratic form of X . The affine part of this quadric visible in the standard chart

$$U_0 = U_{x_0} = \{w \in W \mid x_0(w) = 1\} = e + V$$

can be identified with X , because in every affine coordinate system within U_0 originating at e_0 , the quadric $Q_{\text{aff}} \stackrel{\text{def}}{=} Q \cap U_0$ is given by the equation $q(e + v) = f(v) = 0$ in the vector $v \in V$. We write

$$H_\infty \stackrel{\text{def}}{=} \text{Ann}(x_0) = \mathbb{P}(V) \subset \mathbb{P}(W)$$

for the hyperplane at infinity of the chart U_0 and $Q_\infty \stackrel{\text{def}}{=} Q \cap H_\infty$ for the infinitely distant part of Q . The projective quadric Q_∞ is called the *asymptotic quadric* of X . It is defined in $\mathbb{P}(V) = H_\infty$ by the quadratic form $q|_V = f_2 \in S^2 V^*$, the *leading* quadratic form of X . Passing to projective enhancement transforms the affine classification of quadrics to the projective classification of pairs “projective quadric Q + hyperplane H_∞ ” such that $H \not\subset Q$ and $Q \not\subset H$.

Proposition 17.11 *Let two nonempty affine quadrics $X' = Z(f')$, $X'' = Z(f'') \subset \mathbb{A}(V)$ have projective closures $Q', Q'' \subset \mathbb{P}(W)$. Then X' and X'' are affinely equivalent if and only if there exists a linear projective automorphism $\bar{F} : \mathbb{P}(W) \xrightarrow{\sim} \mathbb{P}(W)$ such that $\bar{F}(Q') = Q''$ and $\bar{F}(H_\infty) = H_\infty$.*

Proof We identify X' and X'' with $Q'_{\text{aff}} = Q' \cap U_0$ and $Q''_{\text{aff}} = Q'' \cap U_0$ respectively. Let us show first that an affine automorphism $\varphi : U_0 \xrightarrow{\sim} U_0$ is the same as a projective automorphism $\bar{F} : \mathbb{P}(W) \xrightarrow{\sim} \mathbb{P}(W)$ sending H_∞ to itself. By definition,⁴⁰ every affine automorphism φ of an affine space $U_0 = e + V$ maps

$$e + v \mapsto f + D_\varphi v \quad \forall v \in V, \quad (17.20)$$

where $f = \varphi(e) \in U_0$ and $D_\varphi : V \xrightarrow{\sim} V$, the differential of φ , is a linear automorphism by Proposition 6.7 on p. 148. Let $F : W \xrightarrow{\sim} W$ be a linear automorphism of $W = \mathbb{k} \oplus V$ determined by the block matrix

$$\begin{pmatrix} 1 & 0 \\ f & D_\varphi \end{pmatrix} : \begin{pmatrix} \lambda \\ v \end{pmatrix} \mapsto \begin{pmatrix} \lambda \\ \lambda f + v \end{pmatrix}, \quad (17.21)$$

where $1 \in \mathbb{k}$, $0 = (0, \dots, 0) \in \mathbb{k}^n$, $n = \dim V$. Clearly, $F(V) = V$, $F(U_0) = U_0$, and $F|_{U_0} = \varphi$. Conversely, given an automorphism $\bar{F} : \mathbb{P}(W) \xrightarrow{\sim} \mathbb{P}(W)$ sending $\mathbb{P}(V)$ to itself, choose a linear isomorphism $F : W \xrightarrow{\sim} W$ that induces \bar{F} . Then the action

⁴⁰See Definition 6.5 on p. 148.

of F on $W = \mathbb{k} \oplus V$ is given by a block matrix of the form

$$\begin{pmatrix} \mu & 0 \\ f & \psi \end{pmatrix},$$

where $\mu \in \mathbb{k}$, $0 = (0, \dots, 0) \in \mathbb{k}^n$, $f \in V$, and $\psi \in \text{End } V$. Since F is invertible, $\mu \neq 0$ and $\psi \in \text{GL}(V)$. If we rescale F without changing \bar{F} in order to get $\mu = 1$, we obtain a map of the form (17.21), which sends U_0 to itself and induces there an affine automorphism (17.20).

Now let $\bar{F} : \mathbb{P}(W) \xrightarrow{\sim} \mathbb{P}(W)$ take Q' to Q'' and send H_∞ to itself. Then \bar{F} maps Q'_{aff} to Q''_{aff} and assigns an affine automorphism of U_0 . Conversely, if $\bar{F}(Q'_{\text{aff}}) = Q''_{\text{aff}}$, then the projective quadrics $F(Q')$ and Q'' coincide outside the projective hyperplane H_∞ . Then they coincide everywhere by Lemma 17.5 below. \square

Lemma 17.5 *Let $H \subset \mathbb{P}_n$ be a hyperplane and $Q \subset \mathbb{P}_n$ a nonempty quadric such that $Q \not\subset H$ and $H \not\subset Q$. If the ground field is infinite, then $Q \cap H$ is uniquely determined by $Q \setminus H$.*

Proof For $n = 1$, the statement is obvious from Corollary 17.5 on p. 435. Consider $n \geq 2$. If $Q = V(q)$ is smooth, then the same arguments as in Proposition 17.10 on p. 444 allow us to find $n + 2$ points in $Q \setminus H$ such that no $n + 1$ of them lie within a hyperplane. These $n + 2$ points completely determine the polarity

$$\bar{q} : \mathbb{P}(V) \rightarrow \mathbb{P}(V^*),$$

which fixes the equation of Q up to proportionality. If Q is not smooth but has some smooth point $a \in Q \setminus H$, let $L \ni a$ be the projective subspace complementary to $\text{Sing } Q$. By Theorem 17.3 on p. 437, Q is the linear join of $\text{Sing } Q$ and a smooth quadric $Q' = Q \cap L$, which satisfies, together with the hyperplane $H' = H \cap L$, the conditions of the lemma formulated within L . As we have seen already, $Q' \cap H'$ is recovered from $Q' \setminus H'$. Further, $\text{Sing } Q \cap H$ is recovered from $Q \setminus H$, because each line (a, b) with $b \in \text{Sing } Q \cap H$ lies in Q , and all points of this line except for b are in $Q \setminus H$. Since both Q' and $\text{Sing } Q$ are recovered from $Q \setminus H$, their linear join is recovered too. Finally, let all the points of $Q \setminus H$ be singular. Then Q has no smooth points in H as well, because otherwise, every line (ab) with smooth $a \in H$ and singular $b \in Q \setminus H$ lies on Q , and all its points except for a, b are smooth and lie outside H . Thus in this case, $Q = \text{Sing } Q$ is a projective subspace not lying in H , and therefore $Q \cap H$ is completely determined by $Q \setminus H$. \square

The classification of affine quadrics breaks them into four classes: smooth central quadrics, paraboloids, simple cones, and cylinders in accordance with the smoothness singularity of their projective closures Q and the positional relationship between Q and the hyperplane at infinity H_∞ .

17.5.2 Smooth Central Quadrics

An affine quadric $X = V(f)$ is called *smooth central* if its projective closure Q is smooth and the hyperplane at infinity H_∞ is not tangent to Q . In this case, the asymptotic quadric $Q_\infty = Q \cap H_\infty$ is smooth by Proposition 17.7. In the language of equations, X is smooth central if and only if its extended quadratic form (17.19) and leading quadratic form f_2 both have nonzero Gram determinants. The epithet “central” is explained as follows. Write $c \in \mathbb{P}(W)$ for the pole of H_∞ with respect to Q . Since H_∞ is not tangent to Q , $c \in U_0 \setminus Q_{\text{aff}}$. Given a line $\ell = (cd)$ joining c with some point $d \in H_\infty \setminus Q$ and intersecting Q in points $a, b \in Q_{\text{aff}}$, then by Proposition 17.8, the cross ratio $[d, c, b, a]$ is equal to -1 . This means⁴¹ that in the affine part $U_0 \cap \ell = \ell \setminus d$ of this line, the point c is the midpoint of $[a, b]$, i.e., a central smooth affine quadric is centrally symmetric with respect to the pole of the hyperplane at infinity. For this reason, c is called the *center* of the quadric. In every affine coordinate system in U_0 , originating at c , the polynomial f that defines $X = Q_{\text{aff}}$ has no linear term and is of the form $f(x) = f_0 + f_2(x)$, where $f_0 \neq 0$.

Exercise 17.17 Check this.

In an orthogonal basis for f_2 in V , the affine equation for Q_{aff} , on dividing both sides by f_0 , takes the form

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = 1. \quad (17.22)$$

Over an algebraically closed field, it can be simplified to

$$x_1^2 + x_2^2 + \cdots + x_n^2 = 1$$

by rescaling the variables. Hence, all smooth central affine quadrics over an algebraically closed field are affinely equivalent. Over \mathbb{R} , the equation (17.22) can be simplified to

$$x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+m}^2 = \pm 1, \text{ where } p \geq m, \ p + m = n, \quad (17.23)$$

and for $p = m = n/2$, only $+1$ is allowed⁴² on the right-hand side. Among the quadrics (17.23) there is exactly one that is empty. It has the equation $\sum x_i^2 = -1$ and is called the *imaginary ellipsoid*. There is also exactly one quadric without points at infinity. It has the equation $\sum x_i^2 = 1$ with $m = 0$ and is called the *ellipsoid*.

⁴¹See Sect. 11.6.3 on p. 274.

⁴²For $p = m = n/2$, the equation (17.23) with -1 on the right-hand side is transformed to the same equation with $+1$ by changing the signs of both sides and renumbering the variables.

Exercise 17.18 Check that the ellipsoid is bounded and 0-planar.

All other quadrics (17.23) have $Q_\infty \neq \emptyset$ and are called *hyperboloids*. For $p > m$ and $+1$ on the right-hand side of (17.23), the projective quadric Q has signature $(p, m + 1)$ and therefore is m -planar. For $p > m$ and -1 on the right-hand side of (17.23), the signature of Q is (p, m) , and Q is $(m - 1)$ -planar. For $p = m = n/2$, the planarity of Q equals $n/2$. Thus, the 0-planar quadrics (17.23) are exhausted by the ellipsoid and *hyperboloid of two sheets* $x_1^2 + \cdots + x_{n-1}^2 = x_n^2 - 1$.

Exercise 17.19 Convince yourself that the hyperboloid of two sheets has two connected components, whereas all the other quadrics (17.23) are connected.

The infinitely distant piece $Q_\infty = Q \cap H_\infty$ of the quadric (17.23) is given within $H_\infty = \mathbb{P}(V)$ by the equation

$$x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+m}^2 = 0$$

and is m -planar regardless of the sign on the right-hand side of (17.23). Hence, there are no affinely equivalent quadrics among (17.23).

17.5.3 Paraboloids

An affine quadric $X = V(f)$ is called a *paraboloid* if its projective closure Q is smooth and $H_\infty = T_c Q$ is tangent to Q at some point $c \in Q_\infty$. In this case,⁴³ the asymptotic quadric $Q_\infty = H_\infty \cap Q$ has exactly one singular point, namely c . In terms of equations, $X = V(f)$ is a paraboloid if and only if the Gram determinant of the extended quadratic (17.19) is nonzero, whereas the leading quadratic form f_2 has 1-dimensional kernel, and in this case, the kernel is spanned by the vector c .

Since q is nondegenerate, the isotropic vector c is included in some pair b, c spanning the hyperbolic plane $\Pi \subset W$. Then $W = \Pi \oplus \Pi^\perp$, where $\Pi^\perp \subset V = \text{Ann } x_0$, because $V = c^\perp$. Since $b \notin \text{Ann } x_0$, it follows that $x_0(b) \neq 0$, and we can rescale b, c to a hyperbolic basis $e_0 = \lambda b, e_n = \mu c$ of Π such that $x_0(e_0) = 1$. Write e_1, e_2, \dots, e_{n-1} for an orthogonal basis in Π^\perp and provide U_0 with an affine coordinate system originating at $e_0 \in U_0$ with basis e_1, e_2, \dots, e_n in V . The affine equation for X in this system is

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_{n-1} x_{n-1}^2 = x_n. \quad (17.24)$$

⁴³See Sect. 17.7 on p. 441.

Over an algebraically closed field, it can be simplified to

$$x_1^2 + x_2^2 + \cdots + x_{n-1}^2 = x_n.$$

Thus, all paraboloids of a given dimension are affinely equivalent over an algebraically closed field. Over \mathbb{R} , the equation (17.24) can be simplified to

$$x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+m}^2 = x_n, \text{ where } p \geq m, p + m = n - 1. \quad (17.25)$$

The paraboloid (17.25) is m -planar. Therefore, all paraboloids (17.25) are nonempty and mutually inequivalent. The zero-planar paraboloid $x_1^2 + \cdots + x_{n-1}^2 = x_n$ is called *elliptic*, and all the other paraboloids are called *hyperbolic*.

17.5.4 Simple Cones

An affine quadric $X = V(f)$ is called a *simple cone* if its projective closure Q is singular and the asymptotic quadric Q_∞ is smooth.

Exercise 17.20 Convince yourself that for every singular quadric $Q \subset \mathbb{P}(W)$, the smoothness of $Q_\infty = Q \cap H_\infty$ is equivalent to the emptiness of $\text{Sing } Q \cap H_\infty$.

Since the hyperplane H_∞ does not intersect $\text{Sing } Q$, the latter subspace is 0-dimensional. Therefore, Q has exactly one singular point c , with $c \in U_0$, and X is ruled by the lines joining c with the points of the asymptotic quadric lying at infinity. In the language of equations, this means that the extended quadric (17.19) has a 1-dimensional kernel, whose generator c can be normalized such that $x_0(c) = 1$. If we place the origin of the affine coordinate system in U_0 at c , then both terms f_0, f_1 disappear from f , and X turns out to be given by a nondegenerate homogeneous quadratic form $f_2 \in S^2 V^*$. Passing to its orthogonal basis, we get the equation

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2 = 0. \quad (17.26)$$

Over an algebraically closed field, it can be simplified to

$$x_1^2 + x_2^2 + \cdots + x_n^2 = 0. \quad (17.27)$$

Thus, over an algebraically closed field there is exactly one simple cone up to affine equivalence. Over \mathbb{R} , we get a collection of cones

$$x_1^2 + \cdots + x_p^2 = x_{p+1}^2 + \cdots + x_{p+m}^2, \text{ where } p \geq m \text{ and } p + m = n. \quad (17.28)$$

The homogeneous equation (17.28) defines a projective quadric of planarity $m-1$ in $\mathbb{P}(V)$. Therefore, the affine cone (17.28) is m -planar. Hence, all simple cones (17.28)

are affinely inequivalent. Note that for $m = 0$, the real quadric (17.28) is exhausted by just one point, the origin.

17.5.5 Cylinders

An affine quadric $X = V(f)$ is called a *cylinder* if both the projective closure Q and asymptotic quadric Q_∞ are singular. By Exercise 17.20, this means that

$$\text{Sing } Q \cap H_\infty \neq \emptyset.$$

In terms of equations, an affine quadric X is a cylinder if and only if both forms q and f_2 are degenerate. Take a basis e_1, e_2, \dots, e_n of V such that the vectors e_i with $i > r$ form a basis in $\ker q \cap V$. Then the last $n - r$ coordinates disappear from the equation for X . Thus, X is a direct product of the affine space \mathbb{A}^{n-r} parallel to those coordinates and an affine quadric in \mathbb{A}^r without singularities at infinity. The latter belongs to one of the three groups described above.

Example 17.11 (Real Affine Plane Curves of Second Order) The complete list of nonempty second-order “curves” in \mathbb{R}^2 up to affine equivalence is as follows:

- *ellipse* $x_1^2 + x_2^2 = 1$, a smooth central curve without points at infinity;
- *hyperbola* $x_1^2 - x_2^2 = 1$, a smooth central curve intersecting the line at infinity $x_0 = 0$ in two distinct points $(0 : 1 : 0)$, $(0 : 0 : 1)$;
- *parabola* $x_1^2 = x_2$, a smooth curve tangent to infinity at $(0 : 0 : 1)$;
- *double point* $x_1^2 + x_2^2 = 0$, a simple cone over a smooth empty quadric at infinity;
- *cross* $x_1^2 - x_2^2 = 0$, a simple cone over a smooth nonempty quadric at infinity;
- *parallel lines* $x_1^2 = 1$, a cylinder over two points in \mathbb{A}^1 (that is, over a smooth nonempty 0-dimensional quadric);
- *double line* $x_1^2 = 0$, a cylinder over a double point in \mathbb{A}^1 (that is, over a singular 0-dimensional quadric).

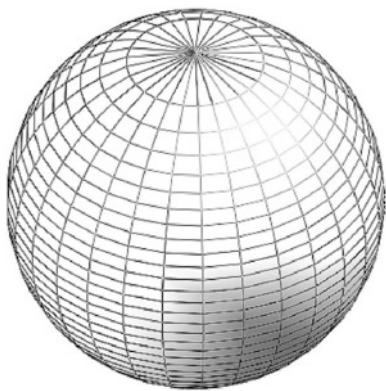
The three smooth curves ellipse, hyperbola, parabola are affine pieces of the same projective conic of signature $(2, 1)$, the Veronese conic.

Example 17.12 (Real Affine Quadratic Surfaces) The complete list of nonempty second-order “surfaces” in \mathbb{R}^3 up to affine equivalence is twice as long. There are three smooth central surfaces:

- *ellipsoid* $x_1^2 + x_2^2 + x_3^2 = 1$, a projective quadric of signature $(3, 1)$ viewed in a chart whose infinite prime does not meet the quadric; the ellipsoid is compact and 0-planar (see Fig. 17.3);
- *hyperboloid of two sheets* $x_1^2 + x_2^2 = x_3^2 - 1$, the same projective quadric of signature $(3, 1)$ but viewed in a chart whose infinite prime crosses the quadric along a smooth conic; the hyperboloid of two sheets is 0-planar and has two connected components (see Fig. 17.4);

Fig. 17.3 Ellipsoid

$$x_1^2 + x_2^2 + x_3^2 = 1$$

**Fig. 17.4** Hyperboloid of

$$\text{two sheets } x_1^2 + x_2^2 = x_3^2 - 1$$



- *hyperboloid of one sheet* $x_1^2 + x_2^2 = x_3^2 + 1$, the Segre quadric, of signature $(2, 2)$, viewed in a chart whose infinite prime crosses the quadric along a smooth conic; the hyperboloid of one sheet is 1-planar and has two line rulings (see Fig. 17.5).

Also, there are two paraboloids:

- *elliptic paraboloid* $x_1^2 + x_2^2 = x_3$, a projective quadric of signature $(3, 1)$ viewed in a chart whose infinite prime touches the quadric at $(0 : 0 : 0 : 1)$ and has no more intersections with it; the elliptic paraboloid is 0-planar (see Fig. 17.6);
- *hyperbolic paraboloid* $x_1^2 - x_2^2 = x_3$, the Segre quadric, of signature $(2, 2)$, viewed in a chart whose infinite prime is tangent to the quadric at $(0 : 0 : 0 : 1)$ and intersects it along two lines $x_1 = \pm x_2$ crossing at the point of tangency the hyperbolic paraboloid is 1-planar and has two line rulings (see Fig. 17.7)

Fig. 17.5 Hyperboloid of one sheet $x_1^2 + x_2^2 = x_3^2 + 1$

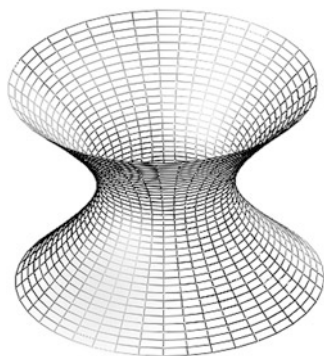


Fig. 17.6 Elliptic paraboloid $x_1^2 + x_2^2 = x_3$

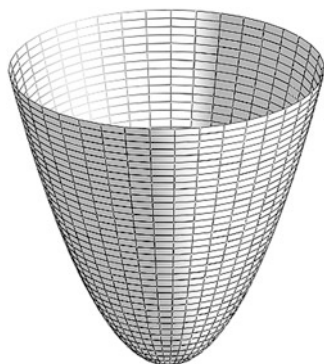


Fig. 17.7 Hyperbolic paraboloid $x_1^2 - x_2^2 = x_3$

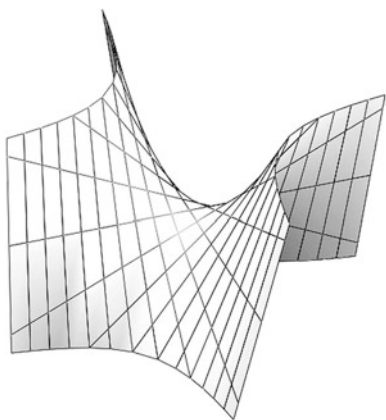


Fig. 17.8 Elliptic cone
 $x_1^2 - x_2^2 = x_3^2$

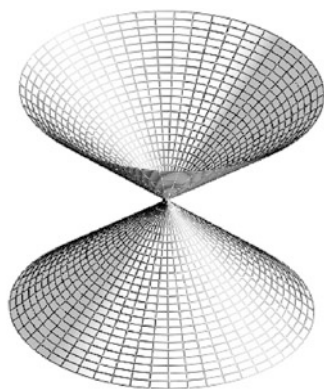
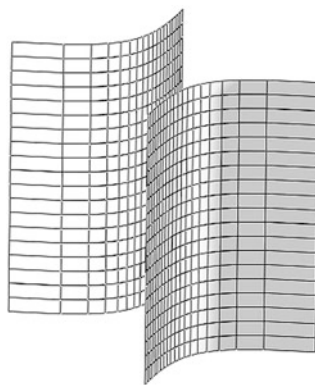


Fig. 17.9 Hyperbolic cylinder
 $x_1^2 - x_2^2 = 1$



There are two simple cones over smooth projective real conics:

- *double point* $x_1^2 + x_2^2 + x_3^2 = 0$, a cone over the empty conic;
- *elliptic cone* $x_1^2 - x_2^2 = x_3^2$, a cone over a nonempty conic (see Fig. 17.8).

Finally, there are seven cylinders over the nonempty second-order “curves” in \mathbb{R}^2 listed in Example 17.11 above. They are given exactly by the same equations but now considered in \mathbb{R}^3 instead of \mathbb{R}^2 . The corresponding surfaces are called elliptic, hyperbolic,⁴⁴ and parabolic cylinders, parallel planes, a double line, intersecting planes, and a double plane. Altogether, we have 14 affinely inequivalent affine quadrics.

⁴⁴See Fig. 17.9.

Problems for Independent Solution to Chap. 17

Problem 17.1 In the standard basis of \mathbb{R}^5 , a symmetric bilinear form β has Gram matrix

$$\begin{pmatrix} -12 & 14 & -5 & -3 & 8 \\ 14 & -17 & 2 & 5 & -8 \\ -5 & 2 & -12 & 3 & 6 \\ -3 & 5 & 3 & -3 & 1 \\ 8 & -8 & 6 & 1 & -6 \end{pmatrix}.$$

- (a) Find the rank and signature for the restriction of β to a subspace given by the linear equations

$$2x_1 + 2x_2 - 3x_3 - 4x_4 - 7x_5 = 0,$$

$$-x_1 - x_2 + 2x_3 + 2x_4 + 4x_5 = 0.$$

- (b) Write an explicit equation for a hyperplane π such that the two lines spanned by the vectors $u = (3, 0, 2, 3, 6)$ and $w = (0, 3, -11, -12, -18)$ are interchanged by the β -orthogonal reflection in π .
- (c) Compute the β -orthogonal projections of u and w on π .

Problem 17.2 Is there a quadratic form on \mathbb{R}^7 with principal upper left minors

(a) $\Delta_1 > 0, \Delta_2 = 0, \Delta_3 > 0, \Delta_4 < 0, \Delta_5 = 0, \Delta_6 < 0, \Delta_7 > 0$;

(b) $\Delta_1 > 0, \Delta_2 = 0, \Delta_3 > 0, \Delta_4 < 0, \Delta_5 = 0, \Delta_6 < 0, \Delta_7 < 0$;

(c) $\Delta_1 > 0, \Delta_2 = 0, \Delta_3 > 0, \Delta_4 < 0, \Delta_5 = 0, \Delta_6 < 0, \Delta_7 < 0$?

If such a form exists, compute its signature and give an explicit example of a Gramian.

Problem 17.3 Find the rank and signature of the quadratic forms $\text{tr}(A^2)$ and $\text{tr}(AA')$ on $\text{Mat}_n(\mathbb{R})$.

Problem 17.4 Expand the characteristic polynomial of the matrix $X \in \text{Mat}_n(\mathbb{R})$ as

$$\det(tE - X) = t^n - \sigma_1(X)t^{n-1} + \sigma_2(X)t^{n-2} + \cdots + (-1)^n \det X.$$

Convince yourself that $\sigma_2(X)$ is a quadratic form on the vector space $\text{Mat}_n(\mathbb{R})$ and find its rank and signature. To begin with, consider $n = 2, 3, 4$.

Problem 17.5 Convince yourself that $A \mapsto \det A$ is a quadratic form on $\text{Mat}_2(\mathbb{k})$ with polarization $\det(A, B) = \text{tr}(AB^\vee)/2$, where B^\vee is the adjunct matrix⁴⁵ of B . Find the rank and signature of this form over $\mathbb{k} = \mathbb{R}$. Is it hyperbolic over $\mathbb{k} = \mathbb{F}_p$?

Problem 17.6 Write W for the space of binary quadratic forms in the variables (x_0, x_1) . For a matrix $A \in \text{GL}_2(\mathbb{k})$, consider the map

$$S_A^2 : W \rightarrow W, f(x_0, x_1) \mapsto f((x_0, x_1) \cdot A).$$

Check that it is linear and write its matrix in the basis $x_0^2, 2x_0x_1, x_1^2$. Express $\text{tr } S^2A$ and $\det S^2A$ in terms of $\text{tr } A$ and $\det A$.

Problem 17.7 Consider the residue ring $K = \mathbb{F}_3[x]/(x^3 - x + 1)$ as a 3-dimensional vector space over \mathbb{F}_3 equipped with a bilinear form $\text{tr}(ab)$, the trace of the multiplication operator $x \mapsto abx$ on K . Write the Gramian of this form in the basis $[1], [x], [x^2]$. Does K contain a hyperbolic plane? If so, write down a hyperbolic basis of this plane explicitly. If not, explain why.

Problem 17.8 Show that the following properties of a vector space W with a nonsingular quadratic form are equivalent: **(a)** W is hyperbolic; **(b)** W is a direct sum⁴⁶ of isotropic subspaces; **(c)** $\dim W$ is even and W contains some isotropic subspace of dimension $\dim W/2$.

Problem 17.9 Write the homogeneous equation of a smooth conic $C \subset \mathbb{P}_2$ in the basis e_0, e_1, e_2 such that the triangle $e_0e_1e_2$ is **(a)** autopolar with respect to C ; **(b)** circumscribed about C ; **(c)** inscribed in C .

Problem 17.10 Given a circle C in the Euclidean plane \mathbb{R}^2 , draw the pole of a given line and the polar of a given point under the polar map provided by C **(a)** using a straightedge and compass; **(b)** using only a straightedge. (Pay especial attention to cases in which the given line does not intersect C and the given point lies inside the disk bounded by C .)

Problem 17.11 Using only a straightedge, draw the tangent line to a given conic C from a given point **(a)** on C ; **(b)** outside C .

Problem 17.12 How many common tangent lines can two different conics on \mathbb{P}_2 over an algebraically closed field have?

Problem 17.13 Given five lines on \mathbb{P}_5 with no three concurrent among them, how many conics touch all of them?

Problem 17.14 Let the vertices a, b, c, d of the complete quadrangle from Example 11.9 on p. 274 lie on some smooth conic C . Show that the associated triangle

⁴⁵See Sect. 9.6 on p. 220.

⁴⁶Summands are not assumed to be orthogonal.

xyz is *autopolar* with respect to C , meaning that its vertices are the poles of the opposite sides.

Problem 17.15 Show that two triangles on \mathbb{P}_2 are perspective⁴⁷ if and only if they are polar to each other with respect to some smooth conic.

Problem 17.16 Show that two triangles in \mathbb{P}_2 are circumscribed about a common conic if and only if they are inscribed in a common conic.

Problem 17.17 (Cross Ratio on a Smooth Conic) For a quadruple a, b, c, d of distinct points on a smooth conic C , write $[a, b, c, d]$ for the cross ratio of lines $[(pa), (pb), (pc), (pd)]$ in the pencil of lines passing through an auxiliary point⁴⁸ $p \in C$. Show that:

- (a) $[a, b, c, d]$ does not depend on⁴⁹ p .
- (b) Two chords $[a, b]$, $[b, c]$ of C are conjugate⁵⁰ with respect to C if and only if $[a, b, c, d] = -1$.
- (c) In Example 17.5 on p. 437, the cross ratio of double points

$$[\{a, a\}, \{b, a\}, \{c, c\}, \{d, d\}]$$

on the Veronese conic $C \subset S^2\mathbb{P}_1$ is equal to the cross ratio $[a, b, c, d]$ on \mathbb{P}_1 .

Problem 17.18 (Segre's Quadric) In the notation of Example 17.6:

- (a) Describe the polarity on $\mathbb{P}(\text{Mat}_2(\mathbb{k}))$ provided by the quadratic form $\det(X)$.
- (b) Show that the operators $\xi \otimes v$ linearly span the vector space $\text{End}(U)$.
- (c) Prove the equivalence of the following properties of an operator $F \in \text{End}(U)$:
 1. $F \in T_{\xi \otimes v} Q_s$;
 2. $F(\text{Ann}(\xi)) \subset \mathbb{k} \cdot v$;
 3. $\exists \eta \in U^*, w \in U : F = \xi \otimes w + \eta \otimes v$.
- (d) Verify that the projective automorphism $\bar{F} : \mathbb{P}(U) \xrightarrow{\sim} \mathbb{P}(U)$ induced by an operator $F \in \text{End}(U) \setminus Q_s$ acts on a point $p = \mathbb{P} \text{Ann}(\xi) \in \mathbb{P}(U)$ as follows. The line $L' = \xi \times \mathbb{P}_1$, which lies in the first ruling family, and the point \bar{F} span a plane in $\mathbb{P}_3 = \mathbb{P}(\text{End}(U))$. This plane intersects Segre's quadric Q_s in a pair of crossing lines $L' \cup L''$, where $L'' = \mathbb{P}_1^\times \times v$ lies in the second ruling family. Then $v = F(p)$.

⁴⁷See Problem 11.12 on p. 276.

⁴⁸Equivalently, we can project C from p onto a line ℓ and write $[a, b, c, d]$ for the cross ratio of the projections.

⁴⁹And on ℓ , if we have used the projection.

⁵⁰That is, a pole of the line (ab) lies on the line (c, d) .

Problem 17.19 Given four nonintersecting lines in (a) $\mathbb{P}(\mathbb{C}^4)$; (b) $\mathbb{A}(\mathbb{C}^4)$; (c) $\mathbb{P}(\mathbb{R}^4)$; (d) $\mathbb{A}(\mathbb{R}^4)$, how many lines intersect all of them? List all possible answers and indicate those that remain unchanged under small perturbations of the given lines.

Problem 17.20 (Plücker Quadric) Write V and W for the spaces of homogeneous linear and quadratic Grassmannian polynomials in the four variables $\xi_1, \xi_2, \xi_3, \xi_4$.

(a) Show that a bilinear form $p : W \times W \rightarrow \mathbb{k}$ is well defined by

$$\omega_1 \wedge \omega_2 = p(\omega_1, \omega_2) \cdot \xi_1 \wedge \xi_2 \wedge \xi_3 \wedge \xi_4$$

and write its Gramian in the basis $\xi_{ij} = \xi_i \wedge \xi_j$, $1 \leq i < j \leq 4$.

- (b) Verify that over every ground field, p is symmetric and nondegenerate and find the signature of p over \mathbb{R} .
- (c) Prove that $\omega \in W$ can be factored as a product of two linear forms if and only if $p(\omega, \omega) = 0$.
- (d) Check that the assignment $(ab) \mapsto a \wedge b$ provides a well-defined bijection between the lines $(ab) \subset \mathbb{P}_3 = \mathbb{P}(V)$ and the points of Plücker's quadric $P = Z(p) \subset \mathbb{P}_5 = \mathbb{P}(W)$.
- (e) Check that two lines in \mathbb{P}_3 intersect if and only if their images in $P \subset \mathbb{P}_5$ are p -orthogonal.
- (f) Show that for every $\omega = a \wedge b \in P$, the intersection $P \cap T_\omega P$ is formed by the images of all lines intersecting the line (ab) .
- (g) Verify that the Plücker quadric is ruled by two families of planes π_Π, π_a , indexed by $\Pi \in \mathbb{P}_3^\times, a \in \mathbb{P}^3$, such that the plane π_Π consists of all lines in \mathbb{P}_3 lying within the plane $\Pi \subset \mathbb{P}_3$, and the plane π_a consists of all lines in \mathbb{P}_3 passing through the point $a \in \mathbb{P}_3$.
- (h) Check that every line on P is uniquely represented as $\pi_\Pi \cap \pi_a$.

Problem 17.21 Find the total number of points over the field⁵¹ \mathbb{F}_9 on (a) the conic $x_0x_1 - x_1x_2 + x_0x_2 = 0$ in \mathbb{P}_2 ; (b) the quadratic surface $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$ in \mathbb{P}_3 .

Problem 17.22 Indicate all ranks and signatures that may have a hyperplane section of a smooth real projective quadric of signature (p, m) .

⁵¹Recall that the field $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1)$ consists of nine elements $a + ib$, where $a, b \in \mathbb{Z}/(3)$ and $i^2 \equiv -1 \pmod{3}$; see Sect. 3.6.2 on p. 63.

Chapter 18

Real Versus Complex

18.1 Realification

18.1.1 Realification of a Complex Vector Space

Let W be a vector space of dimension n over the complex number field \mathbb{C} . Then W can be considered a vector space over the real subfield $\mathbb{R} \subset \mathbb{C}$ as well. The resulting vector space over \mathbb{R} is denoted by $W_{\mathbb{R}}$ and called the *realification* of the complex vector space W . For every basis e_1, e_2, \dots, e_n of W over \mathbb{C} , the vectors $e_1, e_2, \dots, e_n, ie_1, ie_2, \dots, ie_n$ form a basis of $W_{\mathbb{R}}$ over \mathbb{R} , because for every $w \in W$, the uniqueness of the expansion

$$w = \sum (x_v + iy_v) \cdot e_v, \text{ where } (x_v + iy_v) \in \mathbb{C},$$

is equivalent to the uniqueness of the expansion

$$w = \sum x_v \cdot e_v + \sum y_v \cdot ie_v, \text{ where } x_v, y_v \in \mathbb{R}.$$

Therefore, $\dim_{\mathbb{R}} W_{\mathbb{R}} = 2 \dim_{\mathbb{C}} W$. Note that the realification of a complex vector space is always even-dimensional.

18.1.2 Comparison of Linear Groups

Write $\text{End}_{\mathbb{C}}(W)$ for the \mathbb{C} -algebra of all \mathbb{C} -linear maps $F : W \rightarrow W$ and write $\text{End}_{\mathbb{R}}(W_{\mathbb{R}})$ for the \mathbb{R} -algebra of all \mathbb{R} -linear maps $G : W_{\mathbb{R}} \rightarrow W_{\mathbb{R}}$. The first algebra is tautologically embedded in the second as an \mathbb{R} -subalgebra $\text{End}_{\mathbb{C}}(W) \subset \text{End}_{\mathbb{R}}(W_{\mathbb{R}})$.

Let us fix some basis e_1, e_2, \dots, e_n of W over \mathbb{C} and the corresponding basis

$$e_1, e_2, \dots, e_n, ie_1, ie_2, \dots, ie_n \quad (18.1)$$

of $W_{\mathbb{R}}$ over \mathbb{R} and identify $\text{End}_{\mathbb{R}}(W_{\mathbb{R}})$ with $\text{Mat}_{2n}(\mathbb{R})$ by writing the operators as $(2n) \times (2n)$ matrices in the basis (18.1). It is convenient to subdivide such a matrix into four $n \times n$ blocks

$$G = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad (18.2)$$

in accordance with the subdivision of basis vectors (18.1) into two groups of n vectors $\{e_v\}$ and $\{ie_v\}$.

Proposition 18.1 (Cauchy–Riemann Relations) *An operator $G \in \text{End}_{\mathbb{R}}(W_{\mathbb{R}})$ with matrix (18.2) in the basis (18.1) lies in the subalgebra $\text{End}_{\mathbb{C}}(W)$ of $\text{End}_{\mathbb{R}}(W_{\mathbb{R}})$ if and only if $C = B$ and $D = -A$. In this case, G has the complex $n \times n$ matrix $A + iB$ in the basis e_1, e_2, \dots, e_n of W over \mathbb{C} .*

Proof The \mathbb{C} -linearity of G means that $G(iw) = iG(w)$ for all $w \in W_{\mathbb{R}}$. Since this relation is \mathbb{R} -linear in w , it is enough to check it for the basis vectors (18.1) only. This forces $C = B$ and $D = -A$. Conversely, multiplication by the complex matrix $A + iB$ in W acts on the vectors (18.1) by the matrix

$$\begin{pmatrix} A & B \\ -B & A \end{pmatrix}.$$

□

Example 18.1 (Complex-Differentiable Functions) Let $W = \mathbb{C}$. Then $W_{\mathbb{R}} = \mathbb{R}^2$. The basis $e = 1$ of W over \mathbb{C} produces the basis $e = 1, ie = i$ of $W_{\mathbb{R}}$ over \mathbb{R} . Every \mathbb{C} linear operator $F : \mathbb{C} \rightarrow \mathbb{C}$ acts as $w \mapsto zw$ for some $z = a + ib \in \mathbb{C}$, which is nothing but the 1×1 matrix of F in the basis e . In the basis $1, i$ of $W_{\mathbb{R}}$ over \mathbb{R} , the operator \mathbb{F} has real 2×2 matrix

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

An arbitrary (not necessarily linear) map from $\mathbb{C} = \mathbb{R}^2$ to itself can be viewed either as one complex function $w = f(z)$ of one complex variable z or as a pair of real functions of two real variables

$$\begin{cases} u = u(x, y), \\ v = v(x, y), \end{cases} \quad (18.3)$$

related to w and z by the equalities $w = u + iv$, $z = x + iy$. A function $f : \mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto w = f(z)$, is called *complex-differentiable* at a point $z_0 = x_0 + iy_0$ if its increment is approximated by the \mathbb{C} -linear function of the increment of its argument, that is, if

$$f(z_0 + \Delta z) = f(z_0) + \zeta \cdot \Delta z + o(\Delta z) \quad (18.4)$$

for some $\zeta \in \mathbb{C}$. Similarly, a map $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by a pair of functions (18.3) is called *real-differentiable* if its vector increment is approximated by the \mathbb{R} -linear operator acting on the vector increment of the argument, that is, if

$$\begin{pmatrix} u(x_0 + \Delta x, y_0 + \Delta y) \\ v(x_0 + \Delta x, y_0 + \Delta y) \end{pmatrix} = \begin{pmatrix} u(x_0, y_0) \\ v(x_0, y_0) \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix} + o(\Delta x, \Delta y), \quad (18.5)$$

for some matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_{2 \times 2}(\mathbb{R}).$$

It is not hard to check¹ that if the approximations (18.4) and (18.5) exist, then both linear operators² acting on the increments of the arguments are expressed through the derivatives of the functions in question as follows:

$$\zeta = \frac{df}{dz}(z_0) = \lim_{\Delta z \rightarrow 0} \frac{f(z_0 + \Delta z) - f(z_0)}{\Delta z}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{\partial u}{\partial x}(x_0, y_0) & \frac{\partial v}{\partial x}(x_0, y_0) \\ \frac{\partial u}{\partial y}(x_0, y_0) & \frac{\partial v}{\partial y}(x_0, y_0) \end{pmatrix},$$

where

$$\begin{aligned} \frac{\partial u}{\partial x}(x_0, y_0) &= \lim_{\Delta x \rightarrow 0} \frac{u(x_0 + \Delta x, y_0) - f(x_0, y_0)}{\Delta x}, \\ \frac{\partial u}{\partial y}(x_0, y_0) &= \lim_{\Delta y \rightarrow 0} \frac{u(x_0, y_0 + \Delta y) - f(x_0, y_0)}{\Delta y}, \end{aligned}$$

etc. We conclude from Proposition 18.1 that a pair of real differentiable functions (18.3) defines a complex-differentiable map $\mathbb{C} \rightarrow \mathbb{C}$ if and only if these functions satisfy the *differential Cauchy–Riemann equations*

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} \quad \text{and} \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

¹See any calculus textbook.

²They are called *differentials* of the function in question.

18.2 Complexification

18.2.1 Complexification of a Real Vector Space

Every vector space V of dimension n over the field \mathbb{R} admits a canonical extension to a vector space of dimension n over \mathbb{C} called the *complexification* of V and denoted by $V_{\mathbb{C}}$ or $\mathbb{C} \otimes V$. This complex vector space contains the initial real space V in the same manner as the 1-dimensional complex space \mathbb{C} contains the 1-dimensional real space $\mathbb{R} \subset \mathbb{C}$. An explicit construction of $V_{\mathbb{C}}$ is as follows.

Consider one more copy of the space V and denote it by iV to distinguish it from the original. Vectors in the space iV are also denoted by iv . Thus, we have two exemplars of every vector $v \in V$: the original v and its copy $iv \in iV$. Take the direct sum of these spaces and denote it by

$$V_{\mathbb{C}} \stackrel{\text{def}}{=} V \oplus iV. \quad (18.6)$$

This is a vector space over the field \mathbb{R} of dimension $2 \dim_{\mathbb{R}} V$. By construction, it consists of vectors $w = v_1 + iv_2$, and the equality $v_1 + iv_2 = w_1 + iw_2$ in $V_{\mathbb{C}}$ is equivalent to the pair of equalities $v_1 = w_1$, $v_2 = w_2$ in V . Define multiplication by a complex number $z = x + iy \in \mathbb{C}$ in $V_{\mathbb{C}}$ by

$$(x + iy) \cdot (v_1 + iv_2) \stackrel{\text{def}}{=} (xv_1 - yv_2) + i(yv_1 + xv_2) \in V \oplus iV. \quad (18.7)$$

Exercise 18.1 Verify that the multiplication given in (18.7) provides $V_{\mathbb{C}}$ with the structure of a vector space over the field \mathbb{C} .

Note that every basis e_1, e_2, \dots, e_n of V over \mathbb{R} remains a basis of $V_{\mathbb{C}}$ over \mathbb{C} as well, because the existence and uniqueness of expressions of vectors $v_1 \in V$ and $iv_2 \in iV$ respectively in terms of the basis vectors $e_v \in V$ and $ie_v \in iV$ with real coefficients $x_v, y_v \in \mathbb{R}$,

$$v_1 = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n,$$

$$v_2 = y_1 e_1 + y_2 e_2 + \cdots + y_n e_n,$$

means exactly the same as the existence and uniqueness of the expansion of a vector $w = v_1 + iv_2$ in $V_{\mathbb{C}}$ in terms of the vectors e_v with complex coefficients $z_v = x_v + iy_v \in \mathbb{C}$:

$$w = z_1 e_1 + z_2 e_2 + \cdots + z_n e_n.$$

Therefore, $\dim_{\mathbb{C}} V_{\mathbb{C}} = \dim_{\mathbb{R}} V$.

18.2.2 Complex Conjugation

A complexified real vector space $V_{\mathbb{C}}$ is equipped with the \mathbb{R} -linear involution

$$\sigma : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}, \quad w = v_1 + iv_2 \mapsto \overline{w} \stackrel{\text{def}}{=} v_1 - iv_2,$$

called *complex conjugation* and behaving much like complex conjugation of complex numbers within \mathbb{C} . Clearly, $\sigma^2 = \text{Id}_{V_{\mathbb{C}}}$ and the \mathbb{R} -subspaces V , iV are the ± 1 -eigenspaces of σ . The first, which consists of the $+1$ -eigenvectors of σ , is called *real*, whereas the second, consisting of the -1 -eigenvectors of σ , is called *pure imaginary*. Thus, the decomposition $V_{\mathbb{C}} = V \oplus iV$ can be thought of as a diagonalization of σ . Let me stress that σ is *not* \mathbb{C} -linear: $\sigma(zw) = \overline{z}\sigma(w)$ for all $z \in \mathbb{C}$ and all $w \in V_{\mathbb{C}}$. Every \mathbb{R} -linear map between complex vector spaces satisfying this property is called *semilinear* or \mathbb{C} -*antilinear*.

18.2.3 Complexification of Linear Maps

Every \mathbb{R} -linear map $F : V' \rightarrow V''$ between vector spaces over \mathbb{R} can be extended to a \mathbb{C} -linear map between their complexifications:

$$F_{\mathbb{C}} : V'_{\mathbb{C}} \rightarrow V''_{\mathbb{C}}, \quad v_1 + iv_2 \mapsto F(v_1) + iF(v_2). \quad (18.8)$$

The operator $F_{\mathbb{C}}$ is called the *complexification* of the \mathbb{R} -linear operator F .

Exercise 18.2 Verify that $F_{\mathbb{C}}$ is \mathbb{C} -linear, i.e., $F_{\mathbb{C}}(zw) = zF_{\mathbb{C}}(w)$ for all $z \in \mathbb{C}$ and all $w \in V'_{\mathbb{C}}$.

It follows from (18.8) that a complexified operator commutes with complex conjugation of vectors:

$$\overline{F_{\mathbb{C}}(w)} = F_{\mathbb{C}}(\overline{w}) \quad \forall w \in V_{\mathbb{C}}. \quad (18.9)$$

In every basis of $V_{\mathbb{C}}$ formed by real vectors $e_1, e_2, \dots, e_n \in V$, the matrices of F and $F_{\mathbb{C}}$ coincide and are real. In particular, F and $F_{\mathbb{C}}$ have equal characteristic polynomials with real coefficients. The collections of elementary divisors $\mathcal{E}\ell(F)$ and $\mathcal{E}\ell(F_{\mathbb{C}})$ are related by the following proposition.

Proposition 18.2 Every elementary divisor $(t - \lambda)^m \in \mathcal{E}\ell(F)$, where $\lambda \in \mathbb{R}$, is simultaneously an elementary divisor for $F_{\mathbb{C}}$. Every elementary divisor $p^m(t) \in \mathcal{E}\ell(F)$ with monic quadratic trinomial

$$p(t) = t^2 - 2t \operatorname{Re} \lambda + |\lambda|^2 = (t - \lambda)(t - \overline{\lambda}) \in \mathbb{R}[t]$$

irreducible over \mathbb{R} splits into a pair of elementary divisors $(t - \lambda)^m, (t - \overline{\lambda})^m \in \mathcal{E}\ell(F_{\mathbb{C}})$.

Proof The complexification of the real vector space $\mathbb{R}[t]/(p^m)$ is the complex vector space $\mathbb{C}[t]/(p^m)$. The multiplication-by- t operator in the first space is complexified to the multiplication-by- t operator in the second. If $p(t) = (t - \lambda)^m$ for some $\lambda \in \mathbb{R}$, then $\mathbb{C}[t]/(p^m)$ remains an indecomposable $\mathbb{C}[t]$ -module of p -torsion. If

$$p(t) = (t - \lambda)(t - \bar{\lambda})$$

for nonreal $\lambda \in \mathbb{C}$, then the $\mathbb{C}[t]$ -module

$$\mathbb{C}[t]/(p^m) = \mathbb{C}[t]/((t - \lambda)^m) \oplus ((t - \bar{\lambda})^m)$$

splits into the direct sum of two indecomposable submodules. \square

18.2.4 Complex Eigenvectors

Since the field \mathbb{C} is algebraically closed, for every \mathbb{R} -linear operator $F : V \rightarrow V$, the complexified operator $F_{\mathbb{C}} : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}$ has nonempty spectrum. For a nonreal eigenvalue $\lambda = a + ib = \varrho \cdot (\cos \varphi + i \sin \varphi) \in \text{Spec } F_{\mathbb{C}} \setminus \mathbb{R}$ and nonzero eigenvector $w = v_1 + iv_2 \in V_{\mathbb{C}}$ such that $F_{\mathbb{C}}(\lambda w) = \lambda F_{\mathbb{C}}(w)$, we have $F(v_1) + iF(v_2) = F_{\mathbb{C}}(v_1 + iv_2) = (a + ib)(v_1 + iv_2) = (av_1 - bv_2) + i(bv_1 + av_2)$. This means that the \mathbb{R} -linear subspace $U \subset V$ spanned by v_1, v_2 is F -invariant and the matrix of $F|_U$ in the generators v_1, v_2 is equal to

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \varrho \cdot \begin{pmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{pmatrix}. \quad (18.10)$$

Note that we have obtained another proof of Proposition 15.1 on p. 366, which states that every \mathbb{R} -linear operator possesses an invariant subspace of dimension 1 or 2.

Since the matrix (18.10) has determinant $|\lambda|^2 \neq 0$, the vectors v_1, v_2 are linearly independent and form a basis of U over \mathbb{R} and of $\mathbb{C} \otimes U$ over \mathbb{C} . Another basis of $\mathbb{C} \otimes U$ over \mathbb{C} is formed by the nonreal complex conjugate eigenvectors $w = v_1 + iv_2$ and $\bar{w} = v_1 - iv_2$ with conjugate eigenvalues $\lambda = a + ib$ and $\bar{\lambda} = a - ib$.

Exercise 18.3 For every \mathbb{R} -linear operator $F : V \rightarrow V$, check that $w = v_1 + iv_2 \in V_{\mathbb{C}}$ is an eigenvector of $F_{\mathbb{C}}$ with eigenvalue λ if and only if $\bar{w} = v_1 - iv_2$ is an eigenvector of $F_{\mathbb{C}}$ with eigenvalue $\bar{\lambda}$.

For $v_1 \neq 0$, the \mathbb{R} -linear span of the vectors w, \bar{w} intersects the \mathbb{R} -linear span of the real vectors v_1, v_2 along the 1-dimensional (over \mathbb{R}) subspace generated by v_1 . For $v_1 = 0$, these two real planes are transversal. The matrix of $F_{\mathbb{C}}$ in the basis w, \bar{w} is diagonal with conjugate eigenvalues $\lambda, \bar{\lambda}$ on the main diagonal.

If the eigenvalue $\lambda \in \text{Spec } F_{\mathbb{C}}$ is real, then $\lambda \in \text{Spec } F$ as well, and the λ -eigenspace of $F_{\mathbb{C}}$ coincides with the complexification of the λ -eigenspace of F in V :

$$W_{\lambda} = \{w \in V_{\mathbb{C}} \mid F_{\mathbb{C}}(w) = \lambda w\} = \mathbb{C} \otimes \{v \in V \mid F(v) = \lambda v\} = \mathbb{C} \otimes V_{\lambda},$$

because the real and imaginary parts of every complex eigenvector $w = v_1 + iv_2 \in W_\lambda$ lie in V_λ , and conversely, every \mathbb{C} -linear combination of real λ -eigenvectors is a λ -eigenvector as well.

18.2.5 Complexification of the Dual Space

For every real vector space V , there are three complex vector spaces naturally associated with the space $V^* = \text{Hom}_{\mathbb{R}}(V, \mathbb{R})$ dual to V over \mathbb{R} . The first is its complexification $\mathbb{C} \otimes V^*$. The second is $\text{Hom}_{\mathbb{C}}(V_{\mathbb{C}}, \mathbb{C})$, the space dual over \mathbb{C} to the complexified space $V_{\mathbb{C}} = \mathbb{C} \otimes V$. The third is $\text{Hom}_{\mathbb{R}}(V, \mathbb{C})$, the space of \mathbb{R} -linear maps $V \rightarrow \mathbb{C}$, where multiplication by complex numbers is given by the rule $\lambda \cdot \varphi : v \mapsto \lambda \cdot \varphi(v)$. In fact, these three complex vector spaces are canonically isomorphic to each other. Indeed, each \mathbb{R} -linear map $\varphi : V \rightarrow \mathbb{C}$ can be written as $v \mapsto \varphi_1(v) + i\varphi_2(v)$, where $\varphi_1 \stackrel{\text{def}}{=} \text{Re } \varphi : V \rightarrow \mathbb{R}$ and $\varphi_2 = \text{Im } \varphi : V \rightarrow \mathbb{R}$ both are \mathbb{R} -linear. The complexified dual space $\mathbb{C} \otimes V^*$ consists of elements $\varphi_1 + i\varphi_2$, $\varphi_1, \varphi_2 \in V^*$, which are multiplied by complex numbers in the same way as with the previous maps $V \rightarrow \mathbb{C}$. Every \mathbb{C} -linear form $\psi : V_{\mathbb{C}} \rightarrow \mathbb{C}$ lying in the complex space dual to $V_{\mathbb{C}}$ yields $\psi(v_1 + iv_2) = \psi(v_1) + i\psi(v_2)$, because of the \mathbb{C} -linearity. Thus, ψ is uniquely determined by the restriction $\varphi = \psi|_V : V \rightarrow \mathbb{C}$ to the real subspace. The latter is an arbitrary \mathbb{R} -linear form.

18.2.6 Complexification of a Bilinear Form

Every \mathbb{R} -bilinear form $\beta : V \times V \rightarrow \mathbb{R}$ on a real vector space V can be extended to a \mathbb{C} -bilinear form $\beta_{\mathbb{C}} : V_{\mathbb{C}} \times V_{\mathbb{C}} \rightarrow \mathbb{C}$ on the complexified space $V_{\mathbb{C}}$ by

$$\beta_{\mathbb{C}}(u_1 + iu_2, v_1 + iv_2) \stackrel{\text{def}}{=} (\beta(u_1, v_1) - \beta(u_2, v_2)) + i(\beta(u_1, v_2) + \beta(u_2, v_1)).$$

The form $\beta_{\mathbb{C}}$ is called the *complexification* of the bilinear form β .

Exercise 18.4 Convince yourself that the identification $V_{\mathbb{C}}^* \simeq \mathbb{C} \otimes V^*$ described above takes both the left and right correlation maps $V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}^*$ provided by the complexified bilinear form $\beta_{\mathbb{C}}$ to the complexifications of the left and right correlation maps $V \rightarrow V^*$ provided by β .

The Gram matrix of $\beta_{\mathbb{C}}$ in a real basis of $V_{\mathbb{C}}$ over \mathbb{C} coincides with the Gramian of β in the same basis of V over \mathbb{R} . If β is (skew) symmetric, then $\beta_{\mathbb{C}}$ is (skew) symmetric as well. Note that a specific real invariant of a symmetric form, the signature, completely disappears after complexification. For example, all nondegenerate symmetric forms become equivalent over \mathbb{C} and produce the same smooth complex projective quadric $Q \subset \mathbb{P}(V_{\mathbb{C}})$ of planarity $[\dim_{\mathbb{R}} V/2]$. The real projective quadric given by the same form in $\mathbb{P}(V)$ can be recovered as the fixed-point set of the action of the complex conjugation map on Q .

18.3 Real Structures

Let W be an arbitrary vector space over \mathbb{C} . Every \mathbb{R} -linear \mathbb{C} -antilinear operator $\sigma : W_{\mathbb{R}} \rightarrow W_{\mathbb{R}}$ such that $\sigma^2 = \text{Id}_W$ is called a *real structure*³ on the complex vector space W . Every vector space W over \mathbb{C} equipped with a real structure σ splits into a direct sum of ± 1 eigenspaces: $W_{\mathbb{R}} = V_+ \oplus V_-$, where both

$$V_+ = \ker(\sigma - \text{Id}) = \text{im}(\sigma + \text{Id}) \quad \text{and} \quad V_- = \ker(\sigma + \text{Id}) = \text{im}(\sigma - \text{Id})$$

are vector spaces over \mathbb{R} only. Since σ is \mathbb{C} -antilinear, multiplication by i and $-i$ within W assigns \mathbb{R} -linear isomorphisms

$$\begin{array}{ccc} & v_+ \mapsto iv_+ & \\ V_+ & \xleftrightarrow{\quad} & V_- \\ & -iv_- \xleftarrow{\quad} v_- & \end{array}$$

inverse to each other. Indeed, $v_+ \in V_+ \Rightarrow \sigma(v_+) = v_+ \Rightarrow \sigma(iv_+) = -i\sigma(v_+) = -iv_+ \Rightarrow iv_+ \in V_-$, and similarly $v_- \in V_- \Rightarrow \sigma(v_-) = -v_- \Rightarrow \sigma(-iv_-) = i\sigma(v_-) = -iv_- \Rightarrow -iv_- \in V_+$. Therefore, every complex vector space equipped with a real structure σ is canonically identified with the complexification of the $+1$ -eigensubspace V_+ of σ , i.e., $W = V_+ \oplus V_- = V_+ \oplus iV_+$, and multiplication by complex numbers within W proceeds exactly as given in formula (18.7) on p. 462.

Let me stress that a real structure is a supplementary quality of a complex vector space. It is not supplied just by the definition. An arbitrary complex vector space, say one-dimensional, spanned by some abstract vector e , provides no way to say what constitutes the real and pure imaginary parts of e . For example, you can declare them to be $\omega \cdot e$ and $i\omega \cdot e$, where $\omega = (-1 + i\sqrt{3})/2$. If a complex vector space W is equipped with a real structure σ , this means precisely that $W = \mathbb{C} \otimes V$ is the complexification of the real vector space $V = \ker(\sigma - \text{Id})$. An abstract complex vector space can be forcedly equipped with a number of real structures leading to different subspaces of real vectors, and there is no a priori preferred one among them.

Example 18.2 (Hermitian Adjoint of Matrices) A real structure on the space of square complex matrices $W = \text{Mat}_n(\mathbb{C})$ is given by *Hermitian conjugation*

$$\sigma_{\dagger} : A \mapsto A^{\dagger} \stackrel{\text{def}}{=} \overline{A}^t,$$

which takes a matrix to its conjugate transpose.

³Or *complex conjugation*.

Exercise 18.5 Check that σ_{\dagger} is an \mathbb{R} -linear \mathbb{C} -antilinear involution.

The real subspace of Hermitian adjunction consists of *Hermitian matrices*

$$\text{Mat}_n^{\text{H}} \stackrel{\text{def}}{=} \{A \in \text{Mat}_n(\mathbb{C}) \mid A = A^{\dagger}\}.$$

This is an n^2 -dimensional vector space over the field \mathbb{R} . Pure imaginary matrices with respect to Hermitian adjunction are called *skew-Hermitian*.⁴ They also form an n^2 -dimensional vector space

$$\text{Mat}_n^{\text{sH}} \stackrel{\text{def}}{=} \{A \in \text{Mat}_n(\mathbb{C}) \mid A = -A^{\dagger}\}$$

over \mathbb{R} . For example, the Hermitian and skew-Hermitian 2×2 matrices look like this:

$$\begin{pmatrix} a & b+ic \\ b-ic & d \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} ia & b+ic \\ -b+ic & id \end{pmatrix},$$

where $a, b, c, d \in \mathbb{R}$. Note that the main diagonal is real for Hermitian matrices and is pure imaginary for skew-Hermitian ones. Multiplication by i takes a Hermitian matrix to a skew-Hermitian matrix and conversely. An arbitrary matrix is a sum of Hermitian and skew-Hermitian parts:

$$A = A_{\text{H}} + A_{\text{sH}}, \text{ where } A_{\text{H}} = (A + A^{\dagger})/2, \quad A_{\text{sH}} = (A - A^{\dagger})/2.$$

18.4 Complex Structures

If a vector space V over the field \mathbb{R} comes as the realification of a vector space W over \mathbb{C} , then $V = W_{\mathbb{R}}$ inherits a distinguished \mathbb{R} -linear automorphism $I : V \rightarrow V$, $v \mapsto iv$, provided by multiplication by $i \in \mathbb{C}$ within W . Clearly, $I^2 = -\text{Id}_V$. Given an arbitrary vector space V over \mathbb{R} , then every \mathbb{R} -linear operator $I : V \rightarrow V$ such that $I^2 = -\text{Id}_V$ is called a *complex structure* on V , because it allows one to define multiplication of vectors $v \in V$ by complex numbers as follows:

$$(x + iy) \cdot v \stackrel{\text{def}}{=} x \cdot v + y \cdot Iv \quad \forall x + iy \in \mathbb{C}, \forall v \in V. \quad (18.11)$$

Exercise 18.6 Verify that (18.11) provides V with the structure of a vector space over the field \mathbb{C} .

We write V_I for V considered as a vector space over \mathbb{C} with multiplication of vectors by complex numbers defined by the formula (18.11). Note that the initial

⁴Or *anti-Hermitian*.

real vector space V is tautologically the realification of V_I . In particular, this forces $\dim V$ to be even.

Now let us make the verification asked in [Exercise 18.6](#) visible without computations. Since the operator I is annihilated by the polynomial

$$t^2 + 1 = (t + i)(t - i),$$

the complexified operator $I_{\mathbb{C}} : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}$ is diagonalizable⁵ and has eigenvalues among $\pm i$. Therefore, $V_{\mathbb{C}}$ splits into a direct sum of $\pm i$ -eigenspaces

$$U_{\pm} = \ker(I_{\mathbb{C}} \mp i \operatorname{Id}_{V_{\mathbb{C}}})$$

if both are nonzero. By formula (18.9) on p. 463, the relations $I_{\mathbb{C}}w = iw$ and $I_{\mathbb{C}}\bar{w} = -i\bar{w}$ are conjugate to each other and therefore equivalent. In other words, complex conjugation of vectors establishes an \mathbb{R} -linear \mathbb{C} -antilinear isomorphism $U_+ \xrightarrow{\sim} U_-$ between the complex $\pm i$ -eigenspaces of $I_{\mathbb{C}}$, that is, $U_- = \overline{U_+}$. In particular, both eigenspaces are nonempty and have the same dimension $\dim_{\mathbb{C}} U_+ = \dim_{\mathbb{C}} U_- = n$. Therefore, $V_{\mathbb{C}} = U_+ \oplus \overline{U_+}$ as a vector space over \mathbb{C} and $\dim_{\mathbb{R}} V = \dim_{\mathbb{C}} V_{\mathbb{C}} = 2 \dim_{\mathbb{C}} U_+ = 2n$. Taking the real part of a vector establishes an \mathbb{R} -linear isomorphism between the complex vector space U_+ and the initial real vector space V :

$$\operatorname{Re} : U_+ \xrightarrow{\sim} V, \quad w \mapsto \operatorname{Re}(w) = \frac{w + \bar{w}}{2}, \quad (18.12)$$

because $U_+ \cap \ker \operatorname{Re} \subset U_+ \cap \overline{U_+} = 0$ and $\dim_{\mathbb{R}} V = \dim_{\mathbb{R}} U_+$. The isomorphism (18.12) allows us to transfer from U_+ to V the multiplication by complex numbers initially residing in U_+ . We put $\lambda \cdot \operatorname{Re}(u) \stackrel{\text{def}}{=} \operatorname{Re}(\lambda u)$ for all $v = \operatorname{Re}(u) \in V$. This certainly makes a vector space over \mathbb{C} from V . Since $iu = I_{\mathbb{C}}u$ for all $u \in U_+$ and $\operatorname{Re} \circ I_{\mathbb{C}} = I \circ \operatorname{Re}$, we get for every $v = \operatorname{Re}(u) \in V$ and $x + iy \in \mathbb{C}$ the formula

$$\begin{aligned} (x + iy) \cdot v &= (x + iy) \cdot \operatorname{Re}(u) \stackrel{\text{def}}{=} \operatorname{Re}(xu + yiu) = x \operatorname{Re}(u) + y \operatorname{Re}(iu) \\ &= x \operatorname{Re}(u) + y \operatorname{Re}(I_{\mathbb{C}}u) = x \operatorname{Re}(u) + y I(\operatorname{Re} u) = xv + yI(v), \end{aligned}$$

which agrees with (18.11). Let us summarize all these observations in a single claim.

Proposition 18.3 *For every vector space V over \mathbb{R} , the following data are in canonical bijection:*

- (1) *multiplication of vectors by complex numbers $\mathbb{C} \times V \rightarrow V$ that makes a vector space over \mathbb{C} from V and forces V to be the realification of this complex vector space,*
- (2) *the \mathbb{R} -linear operator $I : V \rightarrow V$ such that $I^2 = -\operatorname{Id}_V$,*

⁵See Proposition 15.6 on p. 373.

(3) the complex vector subspace $U \subset V_{\mathbb{C}}$ such that $V_{\mathbb{C}} = U \oplus \overline{U}$.

The correspondence (1) \rightarrow (2) sends multiplication $\mathbb{C} \times V \rightarrow V$ to the multiplication-by- i operator $I : v \mapsto iv$. The correspondence (2) \rightarrow (3) sends the operator I to the $(+i)$ -eigenspace $U = U_+ \subset V_{\mathbb{C}}$ of the complexified operator $I_{\mathbb{C}} : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}$. The correspondence (3) \rightarrow (1) transfers the complex vector space structure on U from U to V by means of the \mathbb{R} -linear isomorphism $\text{Re} : U \xrightarrow{\sim} V$, $w \mapsto (w + \overline{w})/2$. \square

18.5 Hermitian Enhancement of Euclidean Structure

18.5.1 Hermitian Structure

For purposes of metric geometry, which concerns lengths, angles, and areas rather than incidence relations between figures and equations, in the world of complex vector spaces more important than the symmetric inner products are the *Hermitian symmetric*⁶ inner products $(*, *) : W \times W \rightarrow \mathbb{C}$, which satisfy the relation

$$(u, w) = \overline{(w, u)}.$$

Hermitian symmetry forces the inner product of a vector with itself to be real: $(w, w) = \overline{(w, w)} \in \mathbb{R}$. Under the assumption that the inner product of every nonzero vector with itself is positive, the presence of the Hermitian inner product allows one to develop metric geometry in a complex vector space quite similarly to what we did in Chap. 10 for real Euclidean vector spaces. We will go into the Hermitian geometry and metric invariants of linear maps in the next chapter. The remainder of the current chapter will be devoted to algebraic properties inherent in the Hermitian inner product itself.

If a conjugate symmetric product (u, w) is \mathbb{C} -linear in the first argument u , then it has to be \mathbb{C} -antilinear in the second argument w , because $(u, zw) = \overline{(zw, v)} = \overline{z(w, v)} = \overline{z} \overline{(w, v)} = \overline{z}(v, w)$. Every \mathbb{R} -bilinear form $W \times W \rightarrow \mathbb{C}$ that is \mathbb{C} -linear in the first argument and \mathbb{C} -antilinear in the second is called *\mathbb{C} -sesquilinear*.

Definition 18.1 (Hermitian Structure) A complex vector space W equipped with a Hermitian symmetric positive \mathbb{R} -bilinear \mathbb{C} -sesquilinear form

$$(*, *) : W \times W \rightarrow \mathbb{C}$$

⁶Or *conjugate symmetric*.

is called *Hermitian*. These conditions mean that $\forall u, w \in W, \forall z \in \mathbb{C}$,

$$\begin{aligned} (u, w) &= \overline{(w, u)} && \text{(Hermitian symmetry),} \\ (zu, w) &= z(u, w) = (u, \bar{z}w) && \text{(sesquilinearity),} \\ (w, w) &> 0 \text{ for } w \neq 0 && \text{(positivity).} \end{aligned} \quad (18.13)$$

Every inner product with such properties is called a *Hermitian structure* on W .

Example 18.3 (Coordinate Space) The *standard Hermitian structure* on the coordinate vector space \mathbb{C}^n is given by

$$(u, w) = u_1 \bar{w}_1 + u_2 \bar{w}_2 + \cdots + u_n \bar{w}_n \quad (18.14)$$

for $u = (u_1, u_2, \dots, u_n), w = (w_1, w_2, \dots, w_n)$. Note that $(w, w) = \sum |w_i|^2 > 0$ for $w \neq 0$.

Example 18.4 (Space of Integrable Functions) The infinite-dimensional analogue of (18.14) is the *standard Hermitian structure* on the space of continuous functions $[a, b] \rightarrow \mathbb{C}$ defined by

$$(f, g) = \int_a^b f(x) \overline{g(x)} dx, \quad (18.15)$$

where the integral of a complex-valued function $h(x) = u(x) + iv(x)$ with $u, v : [a, b] \rightarrow \mathbb{R}$ is defined as

$$\int_a^b h dx = \int_a^b (u(x) + iv(x)) dx \stackrel{\text{def}}{=} \int_a^b u(x) dx + i \int_a^b v(x) dx.$$

Of course, the domain of integration and the notion of integral can be varied here if the positivity condition from (18.13) holds for the class of integrable functions being considered.

Example 18.5 (Hermitian Complexification of Euclidean Space) Let V be a real Euclidean vector space with inner product $(*, *) : V \times V \rightarrow \mathbb{R}$. Then the *standard Hermitian extension* of this product to the complexified space $W = V_{\mathbb{C}}$ is given by the following prescription forced by sesquilinearity:

$$(u_1 + iv_1, u_2 + iv_2)_H \stackrel{\text{def}}{=} ((u_1, u_2) + (v_1, v_2)) + i((u_1, v_2) - (v_1, u_2)). \quad (18.16)$$

Note that the real and imaginary parts on the right-hand side are respectively the symmetric and *skew*-symmetric \mathbb{R} -bilinear forms. Also note that the Hermitian forms in Example 18.3 and Example 18.4 are exactly the standard Hermitian extensions of the standard Euclidean structures considered in Example 10.1 and Example 10.2 on p. 230.

18.5.2 Kähler Triples

The Hermitian structure $(*, *)$ on a complex vector space W assigns three geometric structures at once on the realification $W_{\mathbb{R}}$ of W . These are

- a Euclidean structure $g : W_{\mathbb{R}} \times W_{\mathbb{R}} \rightarrow \mathbb{R}$ provided by $g(u, w) \stackrel{\text{def}}{=} \text{Re}(u, w)$;
- a symplectic form⁷ $\omega : W_{\mathbb{R}} \times W_{\mathbb{R}} \rightarrow \mathbb{R}$, $\omega(u, w) \stackrel{\text{def}}{=} \text{Im}(u, w)$;
- a complex structure $I : w \mapsto iw$.

Indeed, the Hermitian symmetry condition $(u, w) = \overline{(w, u)}$ forces the real and imaginary parts of the product $(u, w) = g(u, w) + i\omega(u, w)$ to satisfy the relations

$$g(u, w) = g(w, u) \quad \text{and} \quad \omega(u, w) = -\omega(w, u).$$

The positivity of the Hermitian inner product implies the inequality $g(v, v) = (v, v) > 0$ for all $v \neq 0$. In particular, g is nondegenerate. The sesquilinearity condition $(u, iw) = -i(u, w)$ forces

$$g(u, Iw) = \omega(u, w) \quad \text{and} \quad \omega(u, Iw) = -g(u, w).$$

In terms of matrices, this means that the Gramians G, Ω of the \mathbb{R} -bilinear forms g, ω and matrix I of the complex structure operator are related by the equality $GI = \Omega$, which allows us to recover any one element of the triple (I, g, ω) from the other two. In particular, it shows that Ω is nondegenerate. Since $(iu, iw) = (u, w)$ by sesquilinearity, we conclude that

$$g(Iu, Iw) = g(u, w) \quad \text{and} \quad \omega(Iu, Iw) = \omega(u, w).$$

In other words, the complex structure operator $I \in \text{O}_g(W_{\mathbb{R}}) \cap \text{Sp}_{\omega}(W_{\mathbb{R}})$ is simultaneously isometric for both forms g, ω .

Definition 18.2 (Kähler Triple) Let V be an even-dimensional real vector space equipped with the data set (I, g, ω) consisting of the complex structure $I : V \rightarrow V$, Euclidean structure $g : V \times V \rightarrow \mathbb{R}$, and symplectic form $\omega : V \times V \rightarrow \mathbb{R}$. Write V_I for the complex vector space constructed from V by means of the complex structure I as in Proposition 18.3 on p. 468. The data set (I, g, ω) is called a *Kähler triple* if the prescription $(u, w) \stackrel{\text{def}}{=} g(u, w) + i\omega(u, w)$ provides V_I with a Hermitian structure.

⁷See Sect. 16.6 on p. 411.

18.5.3 Completing Kähler Triples for a Given Euclidean Structure

Let V be real Euclidean vector space. Write the Euclidean structure on V as

$$g : V \times V \rightarrow \mathbb{R}$$

and let $V_{\mathbb{C}}$ be the complexification of V , and $g_{\mathbb{C}} : V_{\mathbb{C}} \times V_{\mathbb{C}} \rightarrow \mathbb{C}$ the \mathbb{C} -bilinear complexification⁸ of g . The next proposition describes all Kähler triples that complete g up to a Hermitian structure on V .

Proposition 18.4 (Hermitian Completions of a Given Euclidean Structure) *For every (even-dimensional) real Euclidean vector space (V, g) , the following data are in canonical bijection:*

- (1) the Kähler triple (I, g, ω) ,
- (2) the Euclidean isometry $I \in O_g(V)$ such that $I^2 = -\text{Id}_V$,
- (3) the complex vector subspace $U \subset V_{\mathbb{C}}$ that is maximal isotropic for $g_{\mathbb{C}}$.

They are related in the same way as in Proposition 18.3 on p. 468. In particular, the decomposition $V_{\mathbb{C}} = U \oplus \bar{U}$ automatically holds in (3).

Proof As we have seen above, every complex structure $I : V \rightarrow V$ extending g to a Kähler triple must be g -orthogonal. Conversely, given some complex structure $I \in O_g(V)$, the \mathbb{R} -bilinear form $g(v, Iw)$ is nondegenerate and skew-symmetric, because $g(v, Iw) = g(Iv, I^2w) = -g(Iv, w) = -g(w, Iv)$. Therefore, the \mathbb{C} -valued inner product $(v, w) \stackrel{\text{def}}{=} g(v, w) - ig(v, Iw)$ on V is conjugate-symmetric and positive. Since it is \mathbb{C} -linear in the first argument,

$$(Iu, w) = g(Iu, w) + ig(u, w) = i(g(u, w) - ig(Iu, w)) = i(g(u, w) + ig(u, Iw)) = i(u, w),$$

it must be \mathbb{C} -antilinear in the second. Thus, (1) and (2) are in bijection with each other.

Let us show that the correspondence (2) \rightarrow (3) from Proposition 18.3 produces the $g_{\mathbb{C}}$ -isotropic $(+i)$ -eigenspace $U \subset V_{\mathbb{C}}$ of the complexified operator

$$I_{\mathbb{C}} : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}} \text{ if } I \in O_g(V).$$

In a real basis of $V_{\mathbb{C}}$, the orthogonality condition $I^tGI = G$ on I forces $I_{\mathbb{C}}$ to be $g_{\mathbb{C}}$ -orthogonal. Hence for every $u \in U$ such that $I_{\mathbb{C}}u = iu$, we get the equalities $g_{\mathbb{C}}(u, u) = g_{\mathbb{C}}(I_{\mathbb{C}}u, I_{\mathbb{C}}u) = g_{\mathbb{C}}(iu, iu) = -g_{\mathbb{C}}(u, u)$. Therefore, $g_{\mathbb{C}}(u, u) = 0$ for all $(+i)$ -eigenvectors u of $I_{\mathbb{C}}$, as required.

⁸See Sect. 18.2.6 on p. 465.

Now let us show that every $g_{\mathbb{C}}$ -isotropic subspace $U \subset V_{\mathbb{C}}$ has zero intersection with its conjugate \overline{U} . If $u_1 = \overline{u}_2$ for some $u_1, u_2 \in U$, then $u_1 + u_2 \in U$ is real and $g_{\mathbb{C}}$ -isotropic. Since $g_{\mathbb{C}}$ has no real isotropic vectors,⁹ this forces $u_1 = -u_2$. Therefore, $\overline{u}_1 = -\overline{u}_2 = -u_1$ is pure imaginary, that is, $u_1 = iv$ for some $v \in V$. Then $0 = g_{\mathbb{C}}(u_1, u_1) = -g(v, v)$ forces $v = 0$.

Hence, for every maximal $g_{\mathbb{C}}$ -isotropic subspace $U \subset V_{\mathbb{C}}$ of dimension $\dim_{\mathbb{C}} U = \dim_{\mathbb{R}} V$, we have the direct sum decomposition $V_{\mathbb{C}} = U \oplus \overline{U}$. To recover (2) from (3), it remains to show that every operator $I_{\mathbb{C}}$ acting on U and \overline{U} respectively as multiplication by $+i$ and $-i$ is $g_{\mathbb{C}}$ -orthogonal. For every $u = v_1 + iv_2 \in U$ with $v_1, v_2 \in V$, we have

$$\begin{aligned} g_{\mathbb{C}}(\overline{v_1 + iv_2}, \overline{v_1 + iv_2}) &= g(v_1, v_1) - g(v_2, v_2) - 2i g(v_1, v_2) \\ &= \overline{g(v_1, v_1) - g(v_2, v_2) + 2i g(v_1, v_2)} = \overline{g_{\mathbb{C}}(v_1 + iv_2, v_1 + iv_2)} = 0. \end{aligned}$$

Hence, \overline{U} also is $g_{\mathbb{C}}$ -isotropic. Therefore

$$\begin{aligned} g_{\mathbb{C}}(u_1 + \overline{u}_2, u_1 + \overline{u}_2) &= g_{\mathbb{C}}(u_1, \overline{u}_2) + g_{\mathbb{C}}(\overline{u}_1, u_2) = g_{\mathbb{C}}(iu_1, -\overline{u}_2) + g_{\mathbb{C}}(-\overline{u}_1, iu_2) \\ &= g_{\mathbb{C}}(I_{\mathbb{C}}(u_1 + \overline{u}_2), I_{\mathbb{C}}(u_1 + \overline{u}_2)), \end{aligned}$$

as required. \square

Example 18.6 (Hermitian Structures on \mathbb{R}^4) Let g be the standard Euclidean structure on \mathbb{R}^4 . Its Hermitian enhancement turns Euclidean \mathbb{R}^4 to Hermitian \mathbb{C}^2 , preserving the inner product of every vector with itself. By Proposition 18.4, such enhancements (I, g, ω) are in natural bijection with the 2-dimensional isotropic subspaces of the nondegenerate symmetric \mathbb{C} -bilinear form on $\mathbb{C} \otimes \mathbb{R}^4 = \mathbb{C}^4$, that is, with the lines on the Segre quadric¹⁰ in $\mathbb{P}_3 = \mathbb{P}(\mathbb{C}^4)$. Thus, the Euclidean space \mathbb{R}^4 admits two disjoint pencils of Hermitian enhancements. Their explicit geometric description will be given in Sect. 20.2.3 on p. 512 below.

18.6 Hermitian Enhancement of Symplectic Structure

18.6.1 Completing Kähler Triples for a Given Symplectic Structure

Let $\omega : V \times V \rightarrow \mathbb{R}$ be a nondegenerate skew-symmetric \mathbb{R} -bilinear form on an (even-dimensional) vector space V over \mathbb{R} . Write $V_{\mathbb{C}}$ for the complexification of V and $\omega_{\mathbb{C}} : V_{\mathbb{C}} \times V_{\mathbb{C}} \rightarrow \mathbb{C}$ for the \mathbb{C} -bilinear complexification¹¹ of ω . Besides $\omega_{\mathbb{C}}$, we

⁹Because $g_{\mathbb{C}}|_V = g$ is positive anisotropic.

¹⁰See Example 17.6 on p. 439.

¹¹See Sect. 18.2.6 on p. 465.

will also consider the \mathbb{C} -sesquilinear extension of ω to $V_{\mathbb{C}}$ defined by

$$\begin{aligned}\omega_{\mathbb{C}}(u_1 + iw_1, u_2 + iw_2) &\stackrel{\text{def}}{=} \omega_{\mathbb{C}}(u_1 + iw_1, u_2 - iw_2) \\ &= (\omega(u_1, u_2) + \omega(w_1, w_2)) - i(\omega(u_1, w_2) + \omega(u_2, w_1))\end{aligned}\quad (18.17)$$

for all $u_1, u_2, w_1, w_2 \in V$. Note that the $\omega_{\mathbb{H}}$ -inner product of every vector with itself is pure imaginary:

$$\omega_{\mathbb{H}}(u + iw, u + iw) = -2i\omega(u, w).$$

The next proposition describes all Kähler triples completing ω up to a Hermitian structure on V .

Proposition 18.5 (Hermitian Completions of a Given Symplectic Structure)

For every (even-dimensional) real symplectic vector space (V, ω) , the following data are in canonical bijection:

- (1) *the Kähler triple (I, g, ω) ;*
- (2) *the symplectic isometry $I \in \text{Sp}_{\omega}(V)$ satisfying the following two conditions:*
 - (2a) $I^2 = -\text{Id}_V$
 - (2b) *the quadratic form $G(v) \stackrel{\text{def}}{=} -\omega(v, Iv) \in S^2V^*$ is positive anisotropic,*
- (3) *the complex vector subspace $U \subset V_{\mathbb{C}}$ that is the Lagrangian for the symplectic \mathbb{C} -bilinear form $\omega_{\mathbb{C}}$ and is Hermitian with respect to the \mathbb{C} -sesquilinear form $i\omega_{\mathbb{H}}$.*

They are related in the same way as in Proposition 18.3 on p. 468.

Proof The transfers between (1) and (2) are verified exactly as in Proposition 18.4. Namely, every Kähler triple (I, g, ω) has $I \in \text{Sp}_{\omega}(V)$ and positively defined $g(v, v) = -\omega(v, Iv)$, as we know. Conversely, for every symplectic complex structure $I \in \text{Sp}_{\omega}(V)$, $I^2 = -\text{Id}_V$, the \mathbb{R} -bilinear form

$$g : V \times V \rightarrow \mathbb{R}, \quad g(u, w) \stackrel{\text{def}}{=} -\omega(u, Iw),$$

is nondegenerate and symmetric: $\omega(u, Iw) = \omega(Iu, I^2w) = -\omega(Iu, w) = \omega(w, Iu)$. Therefore, the \mathbb{C} -valued form $V \times V \rightarrow \mathbb{C}$ defined by

$$(u, w) \stackrel{\text{def}}{=} g(u, v) + i\omega(u, w) = -\omega(u, Iw) + i\omega(u, w) \quad (18.18)$$

is conjugate-symmetric. Since it is \mathbb{C} -linear in the first argument,

$$\begin{aligned}(Iu, w) &= -\omega(u, w) + i\omega(Iu, w) = i(\omega(Iu, w) + i\omega(u, w)) \\ &= i(-\omega(u, Iw) + i\omega(u, w)) = i(u, w),\end{aligned}$$

it is forced to be \mathbb{C} -antilinear in the second and therefore \mathbb{C} -sesquilinear altogether. It is positive if and only if $(v, v) = -\omega(v, Iv) > 0$ for all nonzero $v \in V$. Therefore, (1) and (2) are in bijection with each other.

The passage (2) \rightarrow (3) described in Proposition 18.3 leads to the Lagrangian $(+i)$ -eigenspace $U \subset V_{\mathbb{C}}$ of $I_{\mathbb{C}}$, because the symplectic operator $I \in \mathrm{Sp}_{\omega}(V)$ has symplectic complexification $I_{\mathbb{C}} \in \mathrm{Sp}_{\omega_{\mathbb{C}}}(V_{\mathbb{C}})$, and hence for all $+i$ -eigenvectors $w_1, w_2 \in U$, we have the equalities

$$\omega_{\mathbb{C}}(w_1, w_2) = \omega_{\mathbb{C}}(I_{\mathbb{C}}w_1, I_{\mathbb{C}}w_2) = \omega_{\mathbb{C}}(iw_1, iw_2) = -\omega_{\mathbb{C}}(w_1, w_2),$$

forcing $\omega_{\mathbb{C}}(w_1, w_2) = 0$. Since for all $u + iv \in U$ with $u, v \in V$ we have $Iu = -v$, the restriction of the sesquilinear form $i\omega_H$ to U looks like this:

$$\begin{aligned}i\omega_H(u_1 + iv_1, u_2 + iv_2) &= \omega(u_1, v_2) - \omega(v_1, v_2) + i(\omega(u_1, u_2) + \omega(v_1, v_2)) \\ &= -\omega(u_1, Iu_2) + \omega(Iu_1, u_2) + i(\omega(u_1, u_2) + \omega(Iu_1, Iu_2)) \\ &= -2\omega(u_1, Iu_2) + 2i\omega(u_1, u_2).\end{aligned}$$

In other words, for every $w_1, w_2 \in U$, we have the following remarkable coincidence:

$$i\omega_H(w_1, w_2) = 2g(\mathrm{Re} w_1, \mathrm{Re} w_2) + 2i\omega(\mathrm{Re} w_1, \mathrm{Re} w_2) = 2(\mathrm{Re} w_1, \mathrm{Re} w_2),$$

where the rightmost term is the inner product (18.18). Hence this product is positive on V if and only if the sesquilinear form $i\omega_H$ is positive on U . In particular, every complex structure satisfying (2) has $+i$ -eigenspace U satisfying (3).

Conversely, for every Lagrangian subspace $U \subset V_{\mathbb{C}}$ such that the real quadratic form $i\omega_H(w, w) = i\omega_{\mathbb{C}}(w, \overline{w})$ is positive on U , the intersection $U \cap \overline{U}$ is equal to zero, because for every $u_1, u_2 \in U$ such that $u_1 = \overline{u_2}$, we have $0 = i\omega_{\mathbb{C}}(u_2, u_1) = i\omega_{\mathbb{C}}(u_2, \overline{u_2}) = i\omega_H(u_2, u_2)$, which forces $u_2 = 0$. Exactly as in Proposition 18.4, the conjugate space \overline{U} is also Lagrangian for $\omega_{\mathbb{C}}$, because for every $w_{1,2} = u_{1,2} + iv_{1,2} \in U$ with $u_{1,2}, v_{1,2} \in V$, we have

$$\omega_{\mathbb{C}}(\overline{w_1}, \overline{w_2}) = \omega_{\mathbb{C}}(u_1 - iv_1, u_2 - iv_2) = \overline{\omega_{\mathbb{C}}(u_1 + iv_1, u_2 + iv_2)} = \overline{\omega_{\mathbb{C}}(w_1, w_2)} = 0.$$

It remains to check that the symplectic form $\omega_{\mathbb{C}}$ is preserved by the operator $I_{\mathbb{C}}$ acting on $V_{\mathbb{C}} = U \oplus \overline{U}$ as multiplication by $+i$ on the first summand and by $-i$ on

the second. This is straightforward:

$$\begin{aligned}\omega_{\mathbb{C}}(u_1 + \bar{v}_1, u_2 + \bar{v}_2) &= \omega_{\mathbb{C}}(u_1, \bar{v}_2) + \omega_{\mathbb{C}}(\bar{v}_1, u_2) \\ &= \omega_{\mathbb{C}}(iu_1, -i\bar{v}_2) + \omega_{\mathbb{C}}(-i\bar{v}_1, iu_2) = \omega_{\mathbb{C}}(I_{\mathbb{C}}(u_1 + \bar{v}_1), I_{\mathbb{C}}(u_2 + \bar{v}_2)).\end{aligned}$$

□

18.6.2 Siegel Upper Half-Space and Riemann Relations

Consider the coordinate space $V = \mathbb{R}^{2n}$ equipped with the standard symplectic form¹² ω , whose Gramian in the standard basis of \mathbb{R}^{2n} is

$$J = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}.$$

Let us write $e'_1, e'_2, \dots, e'_n, e''_1, e''_2, \dots, e''_n$ for this basis. Then both coordinate subspaces V' and V'' spanned by the e'_i and e''_i are Lagrangian, and $V = V' \oplus V''$. The complexified space $V_{\mathbb{C}} = \mathbb{C}^n$ has complexified splitting $V_{\mathbb{C}} = V'_{\mathbb{C}} \oplus V''_{\mathbb{C}}$, where $V'_{\mathbb{C}}, V''_{\mathbb{C}}$ are Lagrangian for the complexified form $\omega_{\mathbb{C}}$.

By Proposition 18.5, the Kähler triples (I, g, ω) completing ω to a Hermitian structure on V are in bijection with the decompositions $V_{\mathbb{C}} = U \oplus \bar{U}$ such that both U and \bar{U} are Lagrangian for $\omega_{\mathbb{C}}$, and $i\omega_{\mathbb{H}}$ is restricted to the positive form on U . For every such decomposition, the first summand U has zero intersection with $V''_{\mathbb{C}}$, because V'' is Lagrangian for $\omega = \omega_{\mathbb{C}}|_V$, and for all $v''_1, v''_2 \in V''$, we have $i\omega_{\mathbb{H}}(v''_1 + iv''_2, v''_1 + iv''_2) = 0$. Therefore, the projection of U onto $V'_{\mathbb{C}}$ along $V''_{\mathbb{C}}$ gives an isomorphism of complex vector spaces $U \cong V'_{\mathbb{C}}$. In particular, there exists a unique basis $\mathbf{w} = (w_1, w_2, \dots, w_n)$ in U projected to $\mathbf{e}' = (e'_1, e'_2, \dots, e'_n)$ along $V''_{\mathbb{C}}$. In matrix notation, this basis is expressed in terms of the standard basis of $V_{\mathbb{C}}$ as

$$(w_1, w_2, \dots, w_n) = (e'_1, \dots, e'_n, e''_1, \dots, e''_n) \cdot \begin{pmatrix} E \\ S \end{pmatrix}, \quad (18.19)$$

where $S \in \text{Mat}_n(\mathbb{C})$. Note that the subspace U is uniquely determined by the matrix S . The Gramians of the restricted forms $\omega_{\mathbb{C}}|_U$ and $i\omega_{\mathbb{H}}|_U$ in the basis $\mathbf{w} = \mathbf{e}' + \mathbf{e}''S$ are equal to

$$(E \ S^t) \cdot \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \cdot \begin{pmatrix} E \\ S \end{pmatrix} = S - S^t \quad \text{and} \quad (E \ S^t) \cdot \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \cdot \begin{pmatrix} E \\ \bar{S} \end{pmatrix} = i(\bar{S} - S^t)$$

¹²See Example 16.3 on p. 393.

respectively. Thus, a complex subspace $U \subset V_{\mathbb{C}}$ is Lagrangian if and only if the matrix S is symmetric. In this case, $i(\bar{S} - S') = \text{Im } S$, and therefore the positivity of $i\omega_H$ on U is equivalent to the positivity of the real symmetric matrix $\text{Im } S$. We come to the following theorem.

Theorem 18.1 *The Kähler triples (I, g, ω) completing the standard symplectic structure ω in \mathbb{R}^{2n} to a Hermitian structure are in bijection with the symmetric complex matrices $S \in \text{Mat}_n(\mathbb{C})$ having positive imaginary part, i.e., satisfying the conditions*

$$S \in \text{Mat}_n(\mathbb{C}), \quad S^t = S, \quad \forall x \in \mathbb{R}^n \searrow 0, \quad x \cdot (\text{Im } S) \cdot x^t > 0. \quad (18.20)$$

The complex structure $I_S : \mathbb{R}^{2n} \rightarrow \mathbb{R}^{2n}$ corresponding to such a matrix $S = X + iY$, $X, Y \in \text{Mat}_n(\mathbb{R})$, has block matrix

$$I_S = \begin{pmatrix} -Y^{-1}X & Y^{-1} \\ -Y - XY^{-1}X & XY^{-1} \end{pmatrix} \quad (18.21)$$

in every symplectic basis of \mathbb{R}^{2n} .

Proof Only formula (18.21) remains to be verified. By Proposition 18.3, the complex structure $I : V \rightarrow V$ coming from the decomposition $V_{\mathbb{C}} = U \oplus \bar{U}$ sends the vector $v = \text{Re } w \in V$ to $I(v) = \text{Re}(iw)$ for every $w \in W$. If $w = e' + e'' \cdot (X + iY)$, then $\text{Re}(w) = e' + e'' \cdot X$ and $\text{Re}(iw) = -e'' \cdot Y$. Therefore,

$$\begin{aligned} I(e'') &= I(\text{Re}(-iw \cdot Y^{-1})) = \text{Re}(w) \cdot Y^{-1} = e' \cdot Y^{-1} + e'' \cdot XY^{-1}, \\ I(e') &= I(\text{Re}(w) - e'' \cdot X) = \text{Re}(iw) - I(e'') \cdot X \\ &= -e' \cdot Y^{-1}X + e'' \cdot (-Y + XY^{-1}X). \end{aligned}$$

□

Remark 18.1 (Notation and Terminology) The locus of all complex matrices satisfying (18.20) is called the *Siegel upper half-space* and is denoted by \mathfrak{H}_n . The name goes back to the case $n = 1$, for which $\text{Mat}_1(\mathbb{C}) = \mathbb{C}$ and $\mathfrak{H}_1 \subset \mathbb{C}$ is exactly the upper half-plane $\text{Im } z > 0$. The constraints (18.20) are known as the *Riemann relations*. They are to be found in several branches of mathematics that appear to be quite far from each other. For example, given a \mathbb{Z} -module $\Lambda \simeq \mathbb{Z}^{2n}$ spanned by the standard n basis vectors in \mathbb{C}^n and n columns of a matrix $S \in \text{Mat}_n(\mathbb{C})$, then the torus $T_{\Lambda} = \mathbb{C}^n / \Lambda$ admits an analytic embedding $T_{\Lambda} \hookrightarrow \mathbb{P}^N$ that identifies T_{Λ} with an algebraic projective variety if and only if the matrix S satisfies the Riemann relations.¹³

¹³For details, see *Tata Lectures on Theta I*, by D. Mumford [Mu] and *Algebraic Curves, Algebraic Manifolds and Schemes*, by V. I. Danilov, V. V. Shokurov [DS].

Problems for Independent Solution to Chap. 18

Problem 18.1 (Conjugate Complex Structure) For a complex vector space W , write \overline{W} for the same abelian group of vectors as W but equipped with another multiplication by complex numbers defined by $z \cdot w \stackrel{\text{def}}{=} \bar{z} \cdot w$. Show that: **(a)** \overline{W} is a vector space over \mathbb{C} , **(b)** $\dim_{\mathbb{C}} \overline{W} = \dim_{\mathbb{C}} W$, **(c)** there is natural \mathbb{C} -linear isomorphism $W \oplus \overline{W} \simeq (W_{\mathbb{R}})_{\mathbb{C}}$, where the right-hand space is the complexified realification of W .

Problem 18.2 Let W be a complex vector space and $F : W \rightarrow W$ a \mathbb{C} -linear operator. Write $F_{\mathbb{C}} : (W_{\mathbb{R}})_{\mathbb{C}} \rightarrow (W_{\mathbb{R}})_{\mathbb{C}}$ for the complexification of the \mathbb{R} -linear operator $F : W_{\mathbb{R}} \rightarrow W_{\mathbb{R}}$ provided by F on the realified vector space $W_{\mathbb{R}}$. How are the characteristic polynomials, eigenvalues, and eigenvectors of F and $F_{\mathbb{C}}$ related?¹⁴

Problem 18.3 Show that for every vector space V over the field \mathbb{R} , the map

$$\mathbb{C} \otimes \text{End}_{\mathbb{R}}(V) \rightarrow \text{End}_{\mathbb{C}}(\mathbb{C} \otimes V), \quad F + iG \mapsto F_{\mathbb{C}} + iG_{\mathbb{C}},$$

is a well-defined \mathbb{C} -linear isomorphism of complex vector spaces.

Problem 18.4 (Hermitian Adjoint Operators) Let a complex vector space W be equipped with the Hermitian inner product (u, w) . Show that for every operator $F \in \text{End}_{\mathbb{C}}(W)$, there exists a unique operator $F^{\dagger} \in \text{End}_{\mathbb{C}}(W)$ such that $(u, Fw) = (F^{\dagger}u, w)$ and $(u, F^{\dagger}w) = (Fu, w)$ for all $u, w \in W$. Check that $(FG)^{\dagger} = G^{\dagger}F^{\dagger}$ and the map $\sigma : F \mapsto F^{\dagger}$ provides the complex vector space $\text{End}_{\mathbb{C}}(W)$ with a real structure.

Problem 18.5 Make a direct computation checking that the matrix I_S from formula (18.21) on p. 477 has $I_S^2 = -E$ and preserves the skew-symmetric form ω .

Problem 18.6 Construct an isomorphism of groups $U_n \simeq \text{O}_{2n}(\mathbb{R}) \cap \text{Sp}_{2n}(\mathbb{R})$.

Problem 18.7 For the realification $W_{\mathbb{R}}$ of the complex vector space W , write $I : W_{\mathbb{R}} \rightarrow W_{\mathbb{R}}$ for the multiplication-by- i operator $w \mapsto iw$ and put

$$\text{End}_{\mathbb{C}}(W_{\mathbb{R}}) \stackrel{\text{def}}{=} \{F \in \text{End}_{\mathbb{R}}(W_{\mathbb{R}}) \mid FI = IF\},$$

$$\text{End}_{\overline{\mathbb{C}}}(W_{\mathbb{R}}) \stackrel{\text{def}}{=} \{F \in \text{End}_{\mathbb{R}}(W_{\mathbb{R}}) \mid FI = -IF\}.$$

Show that $\text{End}_{\mathbb{R}}(W_{\mathbb{R}}) = \text{End}_{\mathbb{C}}(W_{\mathbb{R}}) \oplus \text{End}_{\overline{\mathbb{C}}}(W_{\mathbb{R}})$ and that every $F \in \text{End}_{\mathbb{R}}(W_{\mathbb{R}})$ can be decomposed as $F = C_F + A_F$ with $C_F = (F - IFI)/2 \in \text{End}_{\mathbb{C}}(W_{\mathbb{R}})$, $A_F = (F + IFI)/2 \in \text{End}_{\overline{\mathbb{C}}}(W_{\mathbb{R}})$. Also show that the map $F \mapsto IF$ provides both spaces $\text{End}_{\mathbb{C}}(W_{\mathbb{R}})$ and $\text{End}_{\overline{\mathbb{C}}}(W_{\mathbb{R}})$ with complex structures in which they become

¹⁴Note that $F_{\mathbb{C}}$ acts on a space of twice the dimension of that on which F acts.

a pair of conjugate complex vector spaces in the sense of [Problem 18.1](#), that is, $\text{End}_{\overline{\mathbb{C}}}(W_{\mathbb{R}}) = \overline{\text{End}_{\mathbb{C}}(W_{\mathbb{R}})}$.

Problem 18.8 Under the conditions and notation from [Problem 18.7](#), assume that W is equipped with a Hermitian inner product (u, w) and put $\omega(u, w) = \text{Im}(u, w)$. Check that for every $F \in \text{Sp}_{\omega}(W_{\mathbb{R}})$, its \mathbb{C} -linear component $C_F \in \text{GL}_{\mathbb{C}}(W_{\mathbb{R}}) \subset \text{End}_{\mathbb{C}}(W_{\mathbb{R}})$ is invertible and therefore can be written as $F = C_F(\text{Id}_W + Z_F)$, where $Z_F = C_F^{-1}A_F$. Then prove that (a) $Z_F \in \text{End}_{\overline{\mathbb{C}}}(W_{\mathbb{R}})$, (b) $Z_{F^{-1}} = -C_F Z_F C_F^{-1}$, (c) $C_{F^{-1}} = C_F^{\dagger}$, (d) $F^{-1} = (1 - Z_F)C_F^{\dagger}$, (e) $C_F(1 - Z_F^2)C_F^{\dagger} = \text{Id}_W$, (f) $(u, Z_F w) = (w, Z_F u)$ for all $u, w \in W$, (g) $(w, (1 - Z_F^2)w) > 0$ for all nonzero $w \in W$, (h) $C_{F_1 F_2} = C_{F_1}(\text{Id}_W - Z_{F_1} Z_{F_2}^{-1})C_{F_2}$ and $Z_{F_1 F_2} = C_{F_2}^{-1}(\text{Id}_W - Z_{F_1} Z_{F_2}^{-1})^{-1}(Z_{F_1} - Z_{F_2}^{-1})^{-1}C_{F_2}$ for any $F_1, F_2 \in \text{Sp}_{\omega}(W_{\mathbb{R}})$.

Problem 18.9 Under the conditions and notation from [Problem 18.8](#), write $\mathfrak{B}(W)$ for the set of all pairs $(C, Z) \in \text{GL}_{\mathbb{C}}(W) \times \text{End}_{\overline{\mathbb{C}}}(W_{\mathbb{R}})$ such that $C(1 - Z^2)C^{\dagger} = \text{Id}_W$, $(u, Zw) = (w, Zu)$, for all $u, w \in W$, and $(w, (1 - Z^2)w) > 0$ for all nonzero $w \in W$. Show that the mappings $F \mapsto (C_F, Z_F)$ and $(C, Z) \mapsto C(1 + Z)$ assign the two inverse bijections $\text{Sp}_{\omega}(W_{\mathbb{R}}) \rightleftarrows \mathfrak{B}(W)$.

Problem 18.10 Show that the Siegel upper half-space $\mathfrak{H}_n \subset \text{Mat}_n(\mathbb{C})$ is contractible.¹⁵

¹⁵That is, there exists a continuous map $\gamma : \mathfrak{H}_n \times [0, 1] \rightarrow \mathfrak{H}_n$ whose restrictions to $\mathfrak{H}_n \times \{0\}$ and to $\mathfrak{H}_n \times \{1\}$ are, respectively, the identity map $\text{Id}_{\mathfrak{H}_n}$ and a constant map that sends the whole \mathfrak{H}_n to some point.

Chapter 19

Hermitian Spaces

19.1 Hermitian Geometry

Recall¹ that a vector space W over the field \mathbb{C} is called *Hermitian* if for any two vectors $u, w \in W$, the \mathbb{R} -bilinear *Hermitian inner product* $(u, w) \in \mathbb{C}$ is defined such that

$$(u, w) = \overline{(w, u)}, \quad (zu, w) = z(u, w) = (u, \bar{z}w), \quad \text{and} \quad (w, w) > 0 \text{ for all } w \neq 0.$$

It provides every vector $w \in W$ with a *Hermitian norm*² $\|w\| \stackrel{\text{def}}{=} \sqrt{(w, w)} \in \mathbb{R}_{\geq 0}$. Since

$$\begin{aligned} (u + w, u + w) &= \|u\|^2 + \|w\|^2 + 2 \operatorname{Re}(u, w), \\ (u + iw, u + iw) &= \|u\|^2 + \|w\|^2 - 2i \operatorname{Im}(u, w), \end{aligned}$$

the Hermitian inner product is uniquely recovered from the norm function and the multiplication-by- i operator as

$$2(w_1, w_2) = \|w_1 + w_2\|^2 - \|w_1 + iw_2\|^2. \quad (19.1)$$

Note that this agrees with the general ideology of Kähler triples from Sect. 18.5.2 on p. 471.

¹See Definition 18.1 on p. 469.

²Or just *length* of the vector w ; we use the double vertical bar notation to prevent confusion with the absolute value $|z|$ of a complex number.

19.1.1 Gramians

All the machinery of Gram matrices developed in Sect. 16.1.2 on p. 388 can be perfectly applied to Hermitian inner products considered as \mathbb{R} -bilinear forms. Since the Hermitian product is conjugate-symmetric, for every collection $\mathbf{w} = (w_1, w_2, \dots, w_m)$ of vectors $w_i \in W$, the Gramian of this collection $G_{\mathbf{w}} = ((w_i, w_j))$ is a *Hermitian matrix*,³ that is, it satisfies

$$G_{\mathbf{w}}^t = \overline{G_{\mathbf{w}}}.$$

If one collection of vectors is linearly expressed through another collection as $\mathbf{w} = \nu C_{\nu\mathbf{w}}$ by means of a *complex* transition matrix $C_{\nu\mathbf{w}}$, then the Gramians of those collections are related by

$$G_{\mathbf{w}} = C_{\nu\mathbf{w}}^t \cdot G_{\nu} \cdot \overline{C_{\nu\mathbf{w}}}, \quad (19.2)$$

because the Hermitian product is \mathbb{C} -*antilinear* in the second argument.

Exercise 19.1 Verify formula (19.2).

19.1.2 Gram–Schmidt Orthogonalization Procedure

Let W be a Hermitian space and $\mathbf{u} = (u_1, u_2, \dots, u_m)$ any collection of vectors $u_i \in W$. Exactly as in Euclidean space,⁴ there exists an orthonormal⁵ basis $\mathbf{e} = (e_1, e_2, \dots, e_k)$ in the linear span of the vectors \mathbf{u} such that the transition matrix⁶ $C_{\mathbf{e}\mathbf{u}} = (c_{ij})$ is upper triangular, i.e., has $c_{ij} = 0$ for all $i > j$. An orthonormal basis \mathbf{e} is constructed by the same Gram–Schmidt recursive procedure as in Proposition 10.1 on p. 231.

Exercise 19.2 Verify that it works perfectly.

Lemma 19.1 *For every collection of vectors $\mathbf{w} = (w_1, w_2, \dots, w_m)$, the Gram determinant $\Gamma_{\mathbf{w}} = \det G_{\mathbf{w}}$ is a real nonnegative number vanishing if and only if the vectors are linearly related.*

Proof Let $\mathbf{w} = \mathbf{e} C_{\mathbf{e}\mathbf{w}}$, where $\mathbf{e} = (e_1, e_2, \dots, e_n)$ is an orthonormal basis in the linear span of \mathbf{w} . Then $G_{\mathbf{w}} = C_{\mathbf{e}\mathbf{w}}^t \overline{C_{\mathbf{e}\mathbf{w}}}$. If $n < m$, then $\text{rk } G_{\mathbf{w}} \leq \text{rk } C_{\mathbf{e}\mathbf{w}} \leq n < m$. This

³See Example 18.2 on p. 466.

⁴See Proposition 10.1 on p. 231.

⁵That is, with Gramian $G_{\mathbf{e}} = E$.

⁶Recall that the j th column of $C_{\mathbf{e}\mathbf{u}}$ is formed by the coefficients of the linear expansion of the vector e_j in terms of the vectors \mathbf{u} .

forces $\det G_w = 0$. If $n = m$, then $\det G_w = \det C_{ew} \cdot \overline{\det C_{ew}} = |\det C_{ew}|^2$ is real and positive. \square

19.1.3 Cauchy–Schwarz Inequality

For a collection of two vectors u, w , the previous lemma implies the inequality

$$\det \begin{pmatrix} (u, u) & (u, w) \\ (w, u) & (w, w) \end{pmatrix} = \|u\|^2 \|w\|^2 - (u, w) \cdot \overline{(u, w)} \geq 0,$$

which is an equality if and only if the vectors are proportional. Usually it is written as

$$|(u, w)| \leq \|u\| \cdot \|w\| \quad (19.3)$$

and is called the *Cauchy–Schwarz inequality* or *Cauchy–Bunyakovsky–Schwarz inequality*.

Corollary 19.1 (Triangle Inequality) $\|u\| + \|w\| \geq \|u + w\|$ for all $u, w \in W$.

Proof $\|u + w\|^2 = \|u\|^2 + \|w\|^2 + 2|(u, w)| \leq \|u\|^2 + \|w\|^2 + 2\|u\| \cdot \|w\| = (\|u\| + \|w\|)^2$. \square

19.1.4 Unitary Group

A \mathbb{C} -linear operator $F : W \rightarrow W$ on a Hermitian space W is called *unitary*⁷ if $\|Fw\| = \|w\|$ for all $w \in W$. Formula (19.1) implies that every unitary operator F preserves the inner product:

$$(Fu, Fw) = (u, w) \quad \forall u, w \in W.$$

This forces the matrix of F in any basis to be related to the Gramian of that basis by

$$F^t \cdot G \cdot \overline{F} = G. \quad (19.4)$$

Computation of determinants leads to $|\det F| = 1$. In particular, F is invertible and

$$F^{-1} = \overline{G}^{-1} \overline{F}^t \overline{G} = (G^t)^{-1} \overline{F}^t G^t.$$

In every orthonormal basis, this formula becomes $F^{-1} = \overline{F}^t$.

⁷Or a *Hermitian isometry*.

The unitary operators on W form a group called the *unitary group* of the Hermitian space W and denoted by $U(W)$. Passage to the matrices of operators in some orthonormal basis e_1, e_2, \dots, e_n assigns an isomorphism between $U(W)$ and the group of *unitary matrices*

$$U_n \stackrel{\text{def}}{=} \{F \in GL_n(\mathbb{C}) \mid F^{-1} = \overline{F'}\}.$$

As usual, its subgroup $SU_n \stackrel{\text{def}}{=} SL_n(\mathbb{C}) \cap U_n = \{F \in U_n \mid \det F = 1\}$ is called the *special unitary group*. In contrast with the Euclidean case, the determinant of a nonspecial unitary matrix can take any value on the unit circle

$$U_1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

and does not break isometries into disjoint classes. In other words, there is *no orientation* in Hermitian geometry.

19.1.5 Hermitian Volume

Choose some orthonormal basis $\mathbf{e} = (e_1, e_2, \dots, e_n)$ in W as a unit-volume basis and define the *Hermitian volume* of the parallelepiped spanned by the vectors $\mathbf{v} = \mathbf{e} C_{ev}$ as

$$\text{Vol}(v_1, v_2, \dots, v_n) \stackrel{\text{def}}{=} |\det C|.$$

Since the absolute value of the determinant for the transition matrix between orthonormal bases equals 1, the Hermitian volume does not depend on the choice of orthonormal basis $\mathbf{e} = (e_1, e_2, \dots, e_n)$ in W . Almost the same computation as in the Euclidean case,

$$\text{Vol}^2(v_1, v_2, \dots, v_n) = |\det C_{ev}|^2 = \det C_{ev}' \cdot \overline{\det C_{ev}} = \det G_v,$$

shows that the squared Hermitian volume equals the Gram determinant.

19.1.6 Hermitian Correlation

The Hermitian correlation on a complex Hermitian vector space W takes a vector $w \in W$ to the \mathbb{C} -linear form $hw : W \rightarrow \mathbb{C}, v \mapsto (v, w)$, which depends \mathbb{C} -antilinearly on $w \in W$. This assigns the \mathbb{R} -linear and \mathbb{C} -antilinear map

$$h : W \rightarrow W^*, \quad w \mapsto hw = (*, w). \quad (19.5)$$

Since $hw(w) = (w, w) > 0$, this map is injective. Since $\dim W = \dim W^*$, it is a \mathbb{C} -antilinear isomorphism. Moreover, the Hermitian correlation is symmetric, meaning that its dual map⁸ $h^* : W^{**} \rightarrow W^*$ becomes h under the canonical identification $W^{**} \simeq W$.

Exercise 19.3 Verify that the matrix of the Hermitian correlation in any dual bases \mathbf{e}, \mathbf{e}^* of W, W^* coincides with the Gramian $G_{\mathbf{e}}$ of the basis \mathbf{e} in the sense that h takes the vector $w = \mathbf{e} \cdot x$, where $x \in \mathbb{C}^n$ is a column of coordinates, to the covector $\mathbf{e}^* \cdot y$, where $y = G_{\mathbf{e}} \cdot \bar{x}$.

For a basis $\mathbf{w} = (w_1, w_2, \dots, w_n)$ of W , the preimage $\mathbf{w}^\vee = h^{-1}\mathbf{w}^*$ of the basis \mathbf{w}^* in W^* dual to \mathbf{w} is called the *Hermitian dual* basis to \mathbf{w} . The basis $\mathbf{w}^\vee = (w_1^\vee, w_2^\vee, \dots, w_n^\vee)$ is uniquely determined by the orthogonality relations

$$(w_i, w_j^\vee) = \begin{cases} 1 & \text{for } i = j, \\ 0 & \text{for } i \neq j, \end{cases}$$

and is expressed in terms of \mathbf{w} as $\mathbf{w}^\vee = \mathbf{w} \overline{G_{\mathbf{w}}}^{-1}$.

19.1.7 Orthogonal Projections

Given a subspace $U \subset W$ in Hermitian space W , the subspace

$$U^\perp = \{w \in W \mid \forall u \in U (u, w) = 0\}$$

is called the *orthogonal complement*⁹ to U . The positivity of the inner product implies the transversality $U \cap U^\perp = 0$. Since $\dim U^\perp = \dim h(U^\perp) = \dim \text{Ann } U = \dim W - \dim U$, we conclude that $W = U \oplus U^\perp$. The projection $\pi_U : W \rightarrow U$ along U^\perp is called the *orthogonal projection* onto U . Its action on an arbitrary vector $w \in W$ is described in the same way as in Euclidean space.

Proposition 19.1 *For every $w \in W$, there exists a unique $w_U \in U$ with the following equivalent properties:*

- (1) $w - w_U \in U^\perp$,
- (2) $(w, u) = (w_U, u) \forall u \in U$,
- (3) $\|w - v_U\| < \|w - u\| \forall u \neq w_U \in U$.

⁸It takes a \mathbb{C} -linear form $F : W^* \rightarrow \mathbb{C}$ to the composition $F \circ h : W \rightarrow \mathbb{C}$ and also is \mathbb{C} -antilinear.

⁹Or just the *orthogonal*.

For every pair of Hermitian dual bases u_1, u_2, \dots, u_k and $u_1^\vee, u_2^\vee, \dots, u_k^\vee$ in U ,

$$\pi_U w = w_U = \sum_{i=1}^k (w, u_i^\vee) \cdot u_i. \quad (19.6)$$

Proof Completely the same as the proof of Theorem 10.1 on p. 237. \square

Exercise 19.4 Check this yourself.

19.1.8 Angle Between Two Lines

Recall that in the Euclidean plane, the angle $\varphi = \angle(u, w)$ between two nonzero vectors u, w is defined by

$$\cos \varphi = \frac{(u, w)}{\|u\| \cdot \|w\|}. \quad (19.7)$$

In a Hermitian space, the inner product (u, w) on the right-hand side becomes complex. This problem is circumvented by taking its absolute value. Let us introduce ψ by

$$\cos \psi = \frac{|(u, w)|}{\|u\| \cdot \|w\|} = |(u/\|u\|, w/\|w\|)|. \quad (19.8)$$

In Euclidean geometry, such ψ equals the previous φ for acute φ , but $\psi = \pi - \varphi$ for obtuse φ . Thus, ψ is the smaller of two contiguous angles between intersecting lines spanned by the vectors rather than the angle between the vectors themselves.

In Hermitian geometry, ψ has the same qualitative sense. However, the geometric environment becomes a bit more complicated. In a complex vector space, the vectors u, w span the 2-dimensional *complex* plane \mathbb{C}^2 , whose realification is \mathbb{R}^4 . In real terms, the complex lines $\mathbb{C} \cdot u$ and $\mathbb{C} \cdot w$ are two transversal real planes $\Pi_u \simeq \mathbb{R}^2$ and $\Pi_w \simeq \mathbb{R}^2$ within \mathbb{R}^4 . Note that they do not break \mathbb{R}^4 into disjoint pieces. In Euclidean geometry, the unit direction vectors $e_u = u/\|u\|$, $e_w = w/\|w\|$ on each line are unique up to a sign. In the Hermitian case, these unit vectors can be chosen arbitrarily on two nonintersecting unit circles $\Pi_u \cap S^3$, $\Pi_w \cap S^3$, which are cut out of the unit 3-sphere $S^3 = \{v \in \mathbb{R}^4 \mid \|v\| = 1\}$ by transversal planes Π_u, Π_w . Every pair of such unit vectors $e_u \in \Pi_u \cap S^3$, $e_w \in \Pi_w \cap S^3$ is joined by a short arc of an equatorial unit circle cut out of S^3 by the real plane spanned by e_u, e_w . Standard compactness arguments show that there is some shortest arc among them. The length of this shortest arc is called the *angle* between the complex lines $\mathbb{C}u, \mathbb{C}w$ in the Hermitian space W . Let us show that it is equal to that ψ introduced in formula (19.8).

Write the Hermitian inner product in $\mathbb{R}^4 = \mathbb{C}^2$ as

$$(v_1, v_2) = g(v_1, v_2) + i\omega(v_1, v_2),$$

where $g(v_1, v_2) = \operatorname{Re}(v_1, v_2)$ is the Euclidean structure uniquely predicted by the equality $g(v, v) = \|v\|^2$ for all v . As e_u, e_w run through unit circles, the sum of squares $g^2(e_u, e_w) + \omega^2(e_u, e_w) = |(e_u, e_w)|^2$ is fixed, because the phase shifts

$$e_u \mapsto \lambda e_u, \quad e_w \mapsto \mu e_w$$

with $\lambda, \mu \in \mathbb{C}$, $|\lambda| = |\mu| = 1$ do not change $|(e_u, e_w)|$. The minimal Euclidean angle $\angle(e_u, e_w)$ corresponds to the maximal $\cos^2 \angle(e_u, e_w) = g^2(e_u, e_w)$, that is, to the minimal $\omega^2(v, w)$. The latter equals 0 and is attained, because the 3-dimensional ω -orthogonal

$$e_u^\perp = \{v \in \mathbb{R}^4 \mid \omega(e_u, v) = 0\}$$

has nonzero intersection with the plane Π_w in \mathbb{R}^4 . Thus,

$$|(e_u, e_w)| = \max \cos \angle(e_u, e_w).$$

Note that the Cauchy–Schwarz inequality forces the right-hand side of (19.8) to lie in the segment $[0, 1]$. Therefore, the angle between any two complex lines in a Hermitian space is in the range $0 \leq \psi \leq \pi/2$.

19.2 Adjoint Linear Maps

19.2.1 Hermitian Adjunction

For every \mathbb{C} -linear map of Hermitian spaces $F : U \rightarrow W$, there exists a *Hermitian adjoint* map $F^\dagger : W \rightarrow U$ defined by means of the commutative diagram

$$\begin{array}{ccc} W^* & \xrightarrow{F^*} & U^* \\ h_W \uparrow & & \uparrow h_U \\ W & \xrightarrow{F^\dagger} & U \end{array}, \quad \text{i.e.,} \quad h_U F^\dagger = F^* h_W, \quad (19.9)$$

where h_U, h_W are Hermitian correlations on U, W , and $F^* : W^* \rightarrow U^*$, $\psi \mapsto \psi \circ F$, is the dual map of F . Equivalently, $F^\dagger : W \rightarrow U$ is the unique \mathbb{C} -linear map such that

$$\forall u \in U, \forall w \in W, \quad (Fu, w) = (u, F^\dagger w). \quad (19.10)$$

Exercise 19.5 Verify the equivalence of the conditions (19.9) and (19.10).

If we conjugate both sides in (19.10) and use the conjugate symmetry of the Hermitian inner product, $(v_1, v_2) = \overline{(v_2, v_1)}$, then (19.10) becomes the equivalent requirement

$$\forall u \in U, \forall w \in W, \quad (F^\dagger w, u) = (w, Fu). \quad (19.11)$$

In terms of matrices, the relations (19.9)–(19.11) mean that the matrix F_{wu}^\dagger of the operator F^\dagger in any bases u, w of U, W is related to the matrix F_{uw} of the operator F and Gramians G_u, G_w of the bases by¹⁰

$$F_{uw}^\dagger = \overline{G_u^{-1} F_{uw}^t G_w}. \quad (19.12)$$

For orthonormal bases u, w , this equation is simplified to $F^\dagger = \overline{F}^t$. In particular, $F^{\dagger\dagger} = F$.

Exercise 19.6 Verify that the map $F \mapsto F^\dagger$ is \mathbb{C} -antilinear and $(FG)^\dagger = G^\dagger F^\dagger$.

19.2.2 Adjoint Endomorphisms

For $U = W$, the Hermitian adjunction of operators is a \mathbb{C} -antilinear involution $\text{End}_{\mathbb{C}}(W) \rightarrow \text{End}_{\mathbb{C}}(W)$, $F \mapsto F^\dagger$; that is, it provides the complex vector space $\text{End}_{\mathbb{C}}(W)$ with a *real structure*.¹¹ If we write the operators as matrices in some orthonormal basis of W , then this real structure becomes that considered in Example 18.2 on p. 466. For an arbitrary basis w in W , formula (19.12) says that $F_w^\dagger = \overline{G_w^{-1} F_w^t G_w}$.

Real and pure imaginary operators with respect to Hermitian adjunction are called *self-adjoint*¹² and *anti-self-adjoint*¹³ respectively. They form real¹⁴ vector subspaces

$$\text{End}_{\mathbb{C}}^+(W) = \{F \in \text{End}_{\mathbb{C}}(W) \mid F^\dagger = F\},$$

$$\text{End}_{\mathbb{C}}^-(W) = \{F \in \text{End}_{\mathbb{C}}(W) \mid F^\dagger = -F\},$$

and the realification $\text{End}_{\mathbb{C}}(W)_{\mathbb{R}} = \text{End}_{\mathbb{C}}^+(W) \oplus \text{End}_{\mathbb{C}}^-(W)$ as a vector space over \mathbb{R} . An arbitrary operator can be uniquely decomposed into self-adjoint and anti-self-adjoint components as

$$F = F_+ + F_-$$

where

$$F_+ = \frac{F + F^\dagger}{2} \in \text{End}_{\mathbb{C}}^+(W), \quad F_- = \frac{F - F^\dagger}{2} \in \text{End}_{\mathbb{C}}^-(W).$$

¹⁰Taking into account that $\overline{G_u} = G_u^t$ and $\overline{G_w} = G_w^t$.

¹¹See Sect. 18.3 on p. 466.

¹²Or *Hermitian*.

¹³Or *anti-Hermitian*.

¹⁴That is, over the field \mathbb{R} .

Multiplication by i and $-i$ assigns the inverse \mathbb{R} -linear isomorphisms

$$\text{End}_{\mathbb{C}}^+(W) \xrightleftharpoons[-iF_- \leftarrow F_-]{F_+ \mapsto iF_+} \text{End}_{\mathbb{C}}^-(W).$$

In an orthonormal basis of W , a self-adjoint operator F has a conjugate symmetric matrix $F^t = \overline{F}$, whereas an anti-self-adjoint operator has a conjugate antisymmetric matrix $F^t = -\overline{F}$.

Exercise 19.7 Verify that the unitary operators are exactly those invertible operators whose inverses coincide with the Hermitian adjoint:

$$F \in \text{U}(W) \iff F^\dagger = F^{-1}.$$

19.2.3 Euclidean Adjunction

For a real Euclidean vector space V , we have defined¹⁵ the adjunction of operators $F : V \rightarrow V$ by means of the symmetric correlation $g : V \simeq V^*$ provided by the Euclidean structure. It maps $F \mapsto g^{-1}F^*g$ and is uniquely determined by

$$\forall v_1, v_2 \in V \quad (F^\vee v_1, v_2) = (v_1, Fv_2).$$

In terms of matrices, $F^\vee = G^{-1} \cdot F^t \cdot G$, where G is the Gramian of the Euclidean inner product in the same basis in which the matrix of F is taken. Euclidean adjunction is an involutive antiautomorphism of the \mathbb{R} -algebra $\text{End}_{\mathbb{R}}(V)$. It also leads to a splitting

$$\text{End}_{\mathbb{R}}(V) = \text{End}_{\mathbb{R}}^+(V) \oplus \text{End}_{\mathbb{R}}^-(V), \text{ where } \text{End}_{\mathbb{R}}^\pm(V) = \{F \mid F^\vee = \pm F\},$$

where each $F \in \text{End}_{\mathbb{R}}(V)$ can be decomposed as

$$F = F_+ + F_-, F_\pm = (F \pm F^\vee)/2 \in \text{End}_{\mathbb{R}}^\pm(V).$$

This picture agrees with Hermitian adjunction under complexification. If we equip the complexified space $V_{\mathbb{C}} = \mathbb{C} \otimes V$ with the Hermitian product $(u, w)_{\text{H}}$ provided by the \mathbb{C} -sesquilinear extension of the Euclidean product in V ,

$$(u_1 + iu_2, w_1 + iw_2)_{\text{H}} \stackrel{\text{def}}{=} ((u_1, w_1) + (u_2, w_2)) + i((u_2, w_1) - (u_1, w_2)), \quad (19.13)$$

then every Euclidean orthonormal basis of V over \mathbb{R} is simultaneously an orthonormal basis for the Hermitian space $V_{\mathbb{C}} = \mathbb{C}$ over \mathbb{C} . For every \mathbb{R} -linear operator $F : V \rightarrow V$ and its complexification $F_{\mathbb{C}} : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}$, the relation $(F^\vee)_{\mathbb{C}} = (F_{\mathbb{C}})^\dagger$

¹⁵See Sect. 16.5.3 on p. 411.

holds, because both parts have the same matrix F^t in every real orthonormal basis of V . Therefore, the Euclidean (anti)self-adjoint and orthogonal operators on V , which respectively satisfy $F^\vee = \pm F$ and $F^\vee = F^{-1}$, are complexified to Hermitian (anti)self-adjoint and unitary operators on $V_{\mathbb{C}}$, which satisfy $F^\dagger = \pm F$ and $F^\dagger = F^{-1}$.

Equivalently, we can say that Hermitian adjunction $F \mapsto F^\dagger$ is nothing but the \mathbb{C} -antilinear extension of Euclidean adjunction $F \mapsto F^\vee$ from $\text{End}_{\mathbb{R}}(V)$ onto its complexification¹⁶

$$\mathbb{C} \otimes \text{End}_{\mathbb{R}}(V) \simeq \text{End}_{\mathbb{C}}(V_{\mathbb{C}}).$$

Example 19.1 (Adjoint Linear Differential Operators) Write V for the space of infinitely differentiable functions $f : [a, b] \rightarrow \mathbb{R}$ vanishing together with all derivatives at the endpoints a, b . Introduce a Euclidean inner product on V by the prescription

$$(f, g) = \int_a^b f(t)g(t) dt.$$

Then the differentiation operator $d/dt : f \mapsto f'$ is anti-self-adjoint, as integration by parts shows:

$$\left(\frac{d}{dt}f, g\right) = \int_a^b f'g dt = - \int_a^b fg' dt = \left(f, -\frac{d}{dt}g\right).$$

For every $f \in V$, the multiplication-by- f operator $g \mapsto fg$ is clearly self-adjoint. Keeping in mind that adjunction reverses the composition, we can compute the adjoint operator to any linear differential operator on V . For example, the adjoint operator to $L = t^3 \frac{d^2}{dt^2} : f(t) \mapsto t^3 f''(t)$ is given by

$$f \mapsto (t^3 f)'' = 6tf + 6t^2 f' + t^3 f'',$$

i.e., $L^\vee = t^3 \frac{d^2}{dt^2} + 6t^2 \frac{d}{dt} + 6t$. For a generic second-order operator $L : f \mapsto af'' + bf' + c$, where $a, b, c \in V$, we get similarly $L^\vee = a \frac{d^2}{dt^2} - (b - 2a') \frac{d}{dt} + (c - b' + a'')$.

¹⁶Compare with [Problem 18.3](#) on p. 478.

19.3 Normal Operators

19.3.1 Orthogonal Diagonalization

An operator F on a Hermitian space W is called *normal* if it commutes with its adjoint, i.e., $F^\dagger F = FF^\dagger$. For example, all (anti) self-adjoint operators, which have $F^\dagger = \pm F$, and all unitary operators, which have $F^\dagger = F^{-1}$, are normal.

Theorem 19.1 *An operator F on a Hermitian space W is normal if and only if it can be diagonalized in some orthonormal basis of W . In this case, up to permutations of diagonal elements, the diagonal matrix of F does not depend on the choice of such an orthonormal basis.*

Proof Let the matrix of F in some orthonormal basis be diagonal. Then the matrix of the adjoint operator F^\dagger is also diagonal in this basis and therefore commutes with the matrix of F . Since diagonal elements λ of every diagonal matrix of F are in bijection with the elementary divisors¹⁷ $(t - \lambda) \in \mathcal{EL}(F)$, they do not depend on the choice of basis in which F has a diagonal matrix.

Conversely, let the operator $F : W \rightarrow W$ be normal. For $\dim W = 1$ or scalar $F = \lambda \text{Id}_W$, the operator F is diagonal in every orthonormal basis. For $\dim W > 1$ and nonscalar F , we use induction on $\dim W$. Since the field \mathbb{C} is algebraically closed, a nonscalar operator F has a proper nonzero eigenspace $U \subsetneq W$. Then $W = U \oplus U^\perp$. Since F^\dagger commutes with F , it sends the eigenspace U to itself by Sect. 15.3.3. Therefore, for every $w \in U^\perp$ and all $u \in U$, we have $(Fw, u) = (w, F^\dagger u) = 0$. This means that U^\perp is F -invariant. By the inductive hypothesis, $F|_{U^\perp}$ has a diagonal matrix in some orthonormal basis of U^\perp . We attach to this basis any orthonormal basis of U and get an orthonormal basis for W in which F is diagonal. \square

Corollary 19.2 *A linear operator on a Hermitian space is self-adjoint if and only if it has a real spectrum and can be diagonalized in some orthonormal basis.*

Corollary 19.3 *A linear operator on a Hermitian space is anti-self-adjoint if and only if it has a pure imaginary spectrum and can be diagonalized in some orthonormal basis.*

Corollary 19.4 *A linear operator F on a Hermitian space is unitary if and only if*

$$\text{Spec } F \subset \text{U}_1(\mathbb{C}) = \{z \in \mathbb{C} : |z| = 1\}$$

and F can be diagonalized in some orthonormal basis.

¹⁷Equivalently, we could say that each $\lambda \in \text{Spec } F$ appears on the diagonal exactly $\dim W_\lambda$ times, where $W_\lambda \subset W$ is the λ -eigenspace of F .

Exercise 19.8 Verify that the unitary group U_n is a compact path-connected subset in $\text{Mat}_n(\mathbb{C})$.

19.3.2 Normal Operators in Euclidean Space

An operator F on a real Euclidean space V is called *normal* if it commutes with its Euclidean adjoint, i.e., $F^\vee \cdot F = F \cdot F^\vee$. As we have seen in Sect. 19.2.3, this is equivalent to the normality of the complexified operator $F_{\mathbb{C}}$ on the complexified space $W = V_{\mathbb{C}}$ equipped with the Hermitian structure (19.13) that extends the Euclidean structure by sesquilinearity.

Proposition 19.2 *Every self-adjoint operator F on a real Euclidean space V can be diagonalized in some orthonormal basis. Up to permutation of the diagonal elements, the result of such a diagonalization does not depend on the choice of orthonormal basis.*

Proof Write $W_\lambda = \{w \in V_{\mathbb{C}} \mid F_{\mathbb{C}}w = \lambda w\}$ and $V_\lambda = \{v \in V \mid Fv = \lambda v\}$ for the λ -eigenspaces of $F_{\mathbb{C}}$ and F in $V_{\mathbb{C}}$ and V respectively. By Corollary 19.2, $\text{Spec } F_{\mathbb{C}} = \text{Spec } F$ is real and $V_{\mathbb{C}}$ splits into a direct orthogonal sum:

$$V_{\mathbb{C}} = \bigoplus_{\lambda \in \text{Spec } F_{\mathbb{C}}} W_\lambda. \quad (19.14)$$

In Sect. 18.2.4 on p. 464, we have seen that $W_\lambda = \mathbb{C} \otimes V_\lambda$ for every $\lambda \in \text{Spec } F_{\mathbb{C}} = \text{Spec } F$. Since the complexification of $\bigoplus V_\lambda$ is the whole of $V_{\mathbb{C}}$, we conclude that $\bigoplus V_\lambda$ exhausts the whole of V . \square

Proposition 19.3 *Every anti-self-adjoint operator F on a real Euclidean space V can be written in an appropriate orthonormal basis of V as a block diagonal matrix*

$$\begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_k \end{pmatrix}, \text{ where } A_k = \begin{pmatrix} 0 & a_v \\ -a_v & 0 \end{pmatrix} \text{ and } a_v \in \mathbb{R}.$$

Up to permutation of blocks, the real numbers a_v do not depend on the choice of such an orthonormal basis.

Proof In the notation introduced during the proof of Proposition 19.2, we again have an orthogonal decomposition (19.14), but now all eigenvalues $\lambda \in \text{Spec } F_{\mathbb{C}}$ are pure imaginary. Since the characteristic polynomial $\chi_{F_{\mathbb{C}}} = \chi_F$ has real coefficients, all the eigenvalues of $F_{\mathbb{C}}$ split into conjugate pairs $\pm ia$, $a \in \mathbb{R}$. We have seen in Sect. 18.2.4 that for every such pair, $W_{ia} \oplus W_{-ia} = \mathbb{C} \otimes U$ is the complexification of

some 2-dimensional F -invariant subspace $U \subset V$ on which the restricted operator $F|_U$ has matrix¹⁸

$$\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$$

in every basis v_1, v_2 such that $F_{\mathbb{C}}(v_1 + iv_2) = ia(v_1 + iv_2)$. Then the computation $(v_1, v_2) = (v_1, Fv_1) = -(Fv_1, v_1) = -(v_2, v_1) = -(v_1, v_2)$ forces v_1, v_2 to be orthogonal. It remains to rescale them to unit lengths. \square

Exercise 19.9 Deduce from Corollary 19.4 another independent proof of Theorem 15.2 on p. 370 about the normal form of a Euclidean isometry.

Exercise 19.10 Show that an operator F on a real Euclidean space V is normal if and only if it can be written in an appropriate orthonormal basis of V as a block diagonal matrix that consists of arbitrary 1×1 blocks and 2×2 blocks of the form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Up to permutation of blocks, this matrix does not depend on the choice of orthonormal basis.

Example 19.2 (Euclidean Quadrics) In a Euclidean space V , the real affine quadrics listed in Sect. 17.5 acquire additional metric invariants preserved by orthogonal transformations of the ambient space. These invariants are called *semiaxes* of the Euclidean quadric and are constructed as follows. In Sect. 16.5.4 on p. 411, we have seen that there is a linear bijection between symmetric bilinear forms $\beta : V \times V \rightarrow \mathbb{R}$ and self-adjoint operators $B : V \rightarrow V$. It is given by $\beta(u, w) = (u, Bw)$ for all $u, w \in V$.

Exercise 19.11 Check that in every orthonormal basis of V , the matrix of the operator B coincides with the Gramian of the form β .

Thus, by Proposition 19.2, for every quadratic form $q \in S^2V^*$, there exists an orthonormal basis in V such that $q(x) = a_1x^2_1 + a_2x^2_2 + \cdots + a_rx^2_r$ in the coordinates related to this basis. The coefficients a_i do not depend on the choice of such a basis, because they are equal to the eigenvalues of the unique self-adjoint operator $Q : V \rightarrow V$ such that $\tilde{q}(u, w) = (u, Qw)$ for all $u, w \in V$.

We know from Sect. 17.5.2 on p. 447 that the equation of a smooth central quadric in an affine coordinate system originating at the center of the quadric¹⁹

¹⁸See formula (18.10) on p. 464.

¹⁹Which coincides with the pole of the infinite prime and the unique center of symmetry for the quadric.

looks like $f_2(x) = 1$, where $f_2 \in S^2V^*$. Passing to an orthonormal basis in which f_2 becomes diagonal, we conclude that every smooth central quadric in the Euclidean space \mathbb{R}^n is isometrically congruent to one and only one of the following:

$$a_1^2x_1^2 + \cdots + a_p^2x_p^2 - b_1^2x_{p+1}^2 - \cdots - b_m^2x_{p+m}^2 = \pm 1, \quad (19.15)$$

where $a_i, b_i > 0$, $p \geq m$, $p + m = n$, and for $p = m = n/2$, only $+1$ is allowed on the right-hand side. These quadrics are obtained from those listed in formula (17.23) on p. 447 by axial stretching with real positive magnification coefficients $a_1, a_2, \dots, a_p, b_1, b_2, \dots, b_m$. These coefficients are called the *semiaxes* of the quadric.

For paraboloids,²⁰ the Euclidean structure allows us to indicate a canonical origin for the affine coordinate system as follows. In the notation of Sect. 17.5.3, write $c = H_\infty \cap Q$ for the unique point of Q at infinity and $L = \mathbb{P}(c^\perp) \subset \mathbb{P}(V) = H_\infty$ for the polar of c with respect to the *Euclidean scalar product*. Then L is a projective subspace of codimension 2 in $\mathbb{P}(\mathbb{K} \oplus V)$. The polar line²¹ of L with respect to Q is called the *principal axis of the paraboloid*. By construction, the principal axis passes through c and intersects the paraboloid at one more point within U_0 . This point is called the *vertex of the paraboloid*. In every affine coordinate system originating at the vertex and having the n th coordinate along the principal axis, the equation of the paraboloid is $g(x) = x_n$, where $g = q|_{c^\perp}$ is a nonsingular homogeneous quadratic form, the restriction of the extended quadratic form of the paraboloid on the Euclidean orthogonal complement to c in V .

Exercise 19.12 Check this.

Now we can choose an orthonormal basis in c^\perp where the Gramian of G becomes diagonal and conclude that every paraboloid in the Euclidean space \mathbb{R}^n is isometrically congruent to one and only one of the following:

$$a_1^2x_1^2 + \cdots + a_p^2x_p^2 - b_1^2x_{p+1}^2 - \cdots - b_m^2x_{p+m}^2 = x_n, \quad (19.16)$$

where $a_i, b_i > 0$, $p \geq m$, and $p + m = n - 1$. These quadrics are obtained from those listed in formula (17.25) on p. 449 by axial stretching with magnification coefficients a_i, b_j in the directions perpendicular to the principal axis. The constants a_i, b_i are also called *semiaxes* of the paraboloid.

Cones and cylinders also inherit metric invariants coming from the semiaxes of the nondegenerate quadric that is a base for the cone or cylinder.

²⁰See Sect. 17.5.3 on p. 448.

²¹That is, the locus of poles for all hyperplanes passing through L , or equivalently, the intersection of the polar hyperplanes of all points of L .

19.4 Polar and Singular Value Decompositions

19.4.1 Polar Decomposition

Every nonzero complex number $z \in \text{GL}_1(\mathbb{C})$ can be factored in polar coordinates as $z = \varrho \cdot e^{i\vartheta}$, where $\varrho = |z| = \sqrt{z\bar{z}}$ is real and positive, whereas $e^{i\vartheta} = \cos \vartheta + i \sin \vartheta$ lies in U_1 . A similar factorization can be done for every linear operator $Z \in \text{GL}_n(\mathbb{C})$. The role of ϱ will be played by a self-adjoint operator $S = \sqrt{ZZ^\dagger}$ with positive spectrum. Then $ZS^{-1} \in U_n$. The details are as follows.

Lemma 19.2 *Let $F : U \rightarrow W$ be an arbitrary \mathbb{C} -linear operator between Hermitian spaces. Then both operators $FF^\dagger \in \text{End}(W)$, $F^\dagger F \in \text{End}(U)$ are self-adjoint and have nonnegative spectra. If the operator F is invertible, then the both spectra are strictly positive. Conversely, if FF^\dagger (respectively $F^\dagger F$) has positive spectrum, then F admits some right (respectively left) inverse operator.*

Proof The self-adjointness of both operators is obvious. By Corollary 19.2 on p. 491, it forces their eigenvalues to be real. If $FF^\dagger w = \lambda w \neq 0$ for some $w \in W$, then $F^\dagger w \neq 0$ and $\lambda \cdot (w, w) = (\lambda w, w) = (FF^\dagger w, w) = (F^\dagger w, F^\dagger w)$. Hence, $\lambda = (F^\dagger w, F^\dagger w)/(w, w) > 0$. Similarly, if $F^\dagger F u = \mu u \neq 0$, then $F u \neq 0$ and $\mu = (F u, F u)/(u, u) > 0$. Therefore, the nonzero elements of both spectra are positive. If the operator F is invertible, then $F^\dagger = h_U^{-1} F^* h_W$ is invertible as well. Hence, both operators FF^\dagger , $F^\dagger F$ have zero kernels. Conversely, if $\ker FF^\dagger = 0$, then $(\text{im } F)^\perp = \ker F^\dagger = 0$.

Exercise 19.13 Check that $\ker F^\dagger = (\text{im } F)^\perp$.

Thus, F is surjective and therefore invertible from the right. If $\ker F^\dagger F = 0$, then F is injective and invertible from the left. \square

Theorem 19.2 (Polar Decomposition) *Every invertible \mathbb{C} -linear operator F on a finite-dimensional Hermitian space admits unique factorizations $F = S_1 I_1$ and $F = I_2 S_2$, where the operators U_1, U_2 are unitary, and the operators S_1, S_2 are self-adjoint with strictly positive eigenvalues.*

Proof Choose bases such that FF^\dagger and $F^\dagger F$ are diagonal²² and put $S_1 = \sqrt{FF^\dagger}$, $S_2 = \sqrt{F^\dagger F}$ as the diagonal operators obtained by extraction of the positive square roots from the diagonal elements of the corresponding matrices. Then S_1, S_2 are self-adjoint and have positive eigenvalues as well. By construction, S_1 commutes with FF^\dagger and has $S_1^2 = FF^\dagger$. Similarly, S_2 commutes with $F^\dagger F$ and has $S_2^2 = F^\dagger F$. This forces the operators $I_1 = S_1^{-1} F$ and $I_2 = F S_2^{-1}$ to be unitary, $(I_1 u, I_1 w) = (S_1^{-1} F u, S_1^{-1} F w) = (F^\dagger S_1^{-2} F u, w) = (F^\dagger (FF^\dagger)^{-1} F v, w) = (u, w)$, and similarly, $(I_2 u, I_2 w) = (F S_2^{-1} u, F S_2^{-1} w) = (u, S_2^{-1} F^\dagger F S_2^{-1} w) = (u, F^\dagger F S_2^{-2} w) = (u, w)$. Thus, we have obtained the existence of polar decompositions. Let us show that

²²Such bases may be different for FF^\dagger and $F^\dagger F$ in general.

the factorization $F = S_1 I_1$, where $I_1 \in U(W)$ and S_1 is self-adjoint positive, is unique. Since $I_1^\dagger = I_1^{-1}$, we have $F^\dagger F = S_1^2$. Therefore, S_1 commutes with FF^\dagger . By Proposition 15.8, commuting diagonalizable operators S_1 and FF^\dagger can be diagonalized simultaneously in some common basis. Then the action of S_1 on each μ -eigenspace of FF^\dagger is given by some diagonal matrix whose squared is μE . Since all eigenvalues of S_1 are positive, S_1 must act by the scalar matrix $\sqrt{\mu} E$. Since this completely describes the action of S_1 on the whole space, S_1 is uniquely determined by F . Therefore, $I_1 = FS_1^{-1}$ is unique too. The arguments for $F = I_2 S_2$ are completely symmetric, and we leave them to the reader. \square

Exercise 19.14 Prove that every invertible \mathbb{R} -linear operator F on a real Euclidean space can be uniquely factored as $F = S_1 I_1$ and as $F = I_2 S_2$, where the operators $I_{1,2}$ are orthogonal and the operators $S_{1,2}$ are self-adjoint and have strictly positive eigenvalues.

19.4.2 Exponential Cover of the Unitary Group

The algebra of power series absolutely convergent in all of \mathbb{C} is suitable for evaluation²³ at every operator $F : \mathbb{C}^n \rightarrow \mathbb{C}^n$. In particular, the exponent e^F is well defined for every operator F . If F is anti-self-adjoint with respect to the standard Hermitian structure on \mathbb{C}^n , then $\mathcal{E}(F)$ consists of n linear binomials of the form $t - ia$, $a \in \mathbb{R}$. By Proposition 15.9 on p. 382, $\mathcal{E}(e^F)$ consists of linear binomials $t - e^{ia}$, which are in bijection with the elements of $\mathcal{E}(F)$. We conclude that $e^F : \mathbb{C}^n \rightarrow \mathbb{C}^n$ is a unitary operator with eigenvalues $e^{ia} = \cos a + i \sin a$ that are in bijection²⁴ with the eigenvalues ia of F . Moreover, if we decompose \mathbb{C}^n as a direct sum of 1-dimensional F -invariant subspaces, then they are e^F -invariant as well, and each ia -eigenvector of F is an e^{ia} -eigenvector of e^F . Since every unitary operator can be obtained in this way, we conclude that the *exponential map*

$$\text{End}_{\mathbb{C}}(\mathbb{C}^n) \twoheadrightarrow U_n, \quad F \mapsto e^F, \quad (19.17)$$

is surjective. Therefore, every unitary operator can be written as $I = e^{iT}$ for some self-adjoint operator T . Thus, every $F \in \text{GL}_n(\mathbb{C})$ can be factored as $F = Se^{iT}$, where both S and T are self-adjoint.

Caution 19.1 In contrast with Theorem 19.2, the factorization $F = Se^{iT}$ is not unique, because the exponential map is not injective. For example, $e^{2\pi i \text{Id}} = \text{Id}$. Moreover, the exponential map (19.17) is not a homomorphism, in the sense that $e^{A+B} \neq e^A e^B$ for noncommuting A, B . Instead of such a simple formula, there is a

²³See Sect. 15.4 on p. 379.

²⁴Counting multiplicities.

rather complicated infinite expansion²⁵ of e^{A+B} in terms of the iterated commutators constructed from A, B .

19.4.3 Singular Value Decomposition

The singular value decomposition is a weak bivariant version of the polar decomposition. Let us say that a rectangular matrix $A = (a_{ij})$ is *diagonal* if $a_{ij} = 0$ for all $i \neq j$.

Theorem 19.3 *For every \mathbb{C} -linear map of Hermitian spaces $F : U \rightarrow W$, there exist orthonormal bases of U, W such that the matrix of F in these bases is diagonal with real nonnegative diagonal elements. Up to permutations, the diagonal elements do not depend on the choice of such orthonormal bases.*

Proof Since the endomorphism $F^\dagger F : U \rightarrow U$ is self-adjoint, there exists an orthonormal basis e_1, e_2, \dots, e_n in U formed by the eigenvectors of $F^\dagger F$. By Lemma 19.2, the spectrum of $F^\dagger F$ is real and nonnegative. Therefore, $F^\dagger F e_i = \alpha_i^2 e_i$ for some real $\alpha_i \geq 0$. Let us renumber the basis vectors in order to have $\alpha_i \neq 0$ for $1 \leq i \leq r$ and $\alpha_i = 0$ for all $i > r$. Then for $i > r$, the vector e_i is in $\ker F$, because $F e_i$ is orthogonal to $\operatorname{im} F$: $\forall u \in U, (F e_i, F u) = (F^\dagger F e_i, u) = (0, u) = 0$. At the same time, for $1 \leq i \leq r$, the vectors $F(e_i)$ form an orthogonal system in W :

$$(F e_i, F e_j) = (F^\dagger F e_i, e_j) = \alpha_i^2 (e_i, e_j) = \begin{cases} \alpha_i^2 > 0 & \text{for } 1 \leq i = j \leq r, \\ 0 & \text{for } 1 \leq i \neq j \leq r. \end{cases}$$

Hence, the vectors $f_i = F e_i / \alpha_i$, $1 \leq i \leq r$, form an orthonormal basis in $\operatorname{im} F$.

Exercise 19.15 Verify that f_1, f_2, \dots, f_r span $\operatorname{im} F$.

Let us include the vectors f_i in an orthonormal basis \mathbf{f} for W by attaching some orthonormal basis of $(\operatorname{im} F)^\perp$ to them. Then the matrix $F_{\mathbf{f}\mathbf{e}}$ of the operator F in the bases \mathbf{e}, \mathbf{f} has the required diagonal form. Given another pair of orthonormal bases in which F has a diagonal matrix with r nonzero diagonal elements $\alpha_1, \alpha_2, \dots, \alpha_r$, then $r = \operatorname{rk} F$ is base-independent, and the operator $F^\dagger F$ has the matrix $A^\dagger A = A^t A$, which is diagonal with elements α_i^2 on the diagonal. Thus, the α_i are the nonnegative square roots of the eigenvalues of $F^\dagger F$ and therefore also do not depend on the choice of bases. \square

Exercise 19.16 Prove that for every invertible \mathbb{R} -linear map of Euclidean spaces $F : U \rightarrow W$, there exist orthonormal bases in U, W such that the matrix of F in

²⁵It is known as the *Campbell–Hausdorff series* and can be found in every solid textbook on Lie algebras, e.g., *Lie Groups and Lie Algebras: 1964 Lectures Given at Harvard University*, by J.-P. Serre [Se].

these bases is diagonal with nonnegative diagonal elements, which do not depend, up to permutation, on the choice of such orthonormal bases.

Corollary 19.5 (SVD: Singular Value Decomposition) *Every rectangular complex matrix $F \in \text{Mat}_{m \times n}(\mathbb{C})$ (respectively real matrix $F \in \text{Mat}_{m \times n}(\mathbb{R})$) can be factored as $F = T_m D T_n$, where D is a diagonal $m \times n$ matrix with real nonnegative diagonal elements, and $T_m \in \text{U}_m$, $T_n \in \text{U}_n$ (respectively $T_m \in \text{O}_m$, $T_n \in \text{O}_n$). The diagonal matrix D does not depend on the choice of factorization.*

Definition 19.1 (Singular Values) Given a \mathbb{C} -linear map of Hermitian spaces (respectively \mathbb{R} -linear map of Euclidean spaces) $F : U \rightarrow W$, the diagonal elements α_i of its diagonal matrix from Theorem 19.3 (respectively from Exercise 19.16) are called *singular values* of F . Any zero diagonal elements that may exist are also included. Given a real or complex rectangular matrix F , the diagonal elements of the matrix D from Corollary 19.5 are called *singular values* of the matrix F .

Remark 19.1 Geometrically, Theorem 19.3 and Exercise 19.16 say that every linear map F between real or complex vector spaces equipped with positive inner products can be factored as a dilatation along perpendicular directions (with the direction depending on the stretch coefficients) possibly preceded by the orthogonal projection along the kernel (if $\ker F \neq 0$). Then the nonzero singular values are the stretch coefficients, and the total number of zero singular values is equal to $\dim \ker F$.

Example 19.3 (Euclidean Angles Between Subspaces) Let U, W be two vector subspaces in a real Euclidean vector space, $\dim U = n \leq m = \dim W$. Write $\pi : U \rightarrow W$ for the projection along W^\perp and $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$ for the singular values of π . Since $|\pi u| = |u| \cdot \cos \angle(\pi u, u)$, the numbers $\alpha_i = \cos \varphi_i$ are the cosines of increasing angles

$$0 \leq \varphi_1 \leq \varphi_2 \leq \dots \leq \varphi_n \leq \pi/2, \quad \varphi_i = \angle(w_i, u_i), \quad (19.18)$$

between the first n vectors of some orthonormal basis w_1, w_2, \dots, w_m of W and vectors u_1, u_2, \dots, u_n forming an orthonormal basis of U . By Exercise 19.16, they do not depend on the choice of orthonormal basis in U projected to an orthogonal system of vectors in W . On the other hand, such an orthonormal basis can be constructed geometrically as follows. Choose any orthonormal basis u_1, u_2, \dots, u_{i-1} in $U \cap W$ and put $V_i = (U \cap W)^\perp$, $U_i = U \cap V_i$, $W_i = W \cap V_i$. Then the angle $\angle(u, w)$ between the unit-length vectors $u \in U_i$, $w \in W_i$, $|u| = |w| = 1$, achieves its minimal value at a pair of vectors $u_i \in U_i$, $w_i \in W_i$. This is evident from the compactness of unit spheres and the continuity of $\cos \angle(u, w) = (u, w)$. However, a purely algebraic argument exists as well.

Exercise 19.17 Given two vector subspaces U, W , $\dim U \leq \dim W$, in a Euclidean space, show that the maximum of $\cos \angle(u, w)$ taken over all nonzero $u \in U$, $w \in W$ equals the maximal singular value of the orthogonal projection $U \rightarrow W$.

Now attach u_i and w_i to the bases being constructed, write $V_{i+1} \subset V_i$ for the orthogonal to the plane spanned by u_i, w_i , put $U_{i+1} = U_i \cap V_{i+1}$, $W_{i+1} = W_i \cap V_{i+1}$, and proceed further by induction. We conclude that the (nonstrictly) increasing collection of minimal angles obtained in this way coincides with the singular values of the projection π and does not depend on possible ambiguities in the choice of u_i, w_i at each step. The angles (19.18) form a complete system of invariants for a pair of subspaces in Euclidean space.

Exercise 19.18 Show that one pair of subspaces U', W' can be transformed to another pair of subspaces U'', W'' by an orthogonal automorphism of the ambient Euclidean space if and only if $\dim U' = \dim U'', \dim W' = \dim W''$, and the angles (19.18) for U', W' are the same as for U'', W'' .

For arbitrary orthonormal bases $e = (e_1, e_2, \dots, e_n)$ in U and $f = (f_1, f_2, \dots, f_m)$ in W , the singular values of their reciprocal Gramian²⁶ $G_{ef} = ((e_i, f_j))$ coincide with the cosines $\alpha_i = \cos \varphi_i$ of the angles (19.18), because in passing to the orthonormal bases u, w constructed above, we get a singular value decomposition as in Corollary 19.5: $G_{ef} = C_{ue}^t G_{uw} C_{wf}$, where the Gramian G_{uw} is diagonal, $C_{ue}^t = C_{ue}^{-1} = C_{eu} \in O(U)$, $C_{wf} \in O(W)$.

Problems for Independent Solution to Chap. 19

Problem 19.1 Give an explicit example of an operator F on a Hermitian space W and a proper F -invariant subspace $U \subset W$ such that U^\perp is not F -invariant.

Problem 19.2 Prove that $(\ker F)^\perp = \operatorname{im} F^\dagger$.

Problem 19.3 Let $W = U_1 \oplus U_2$, where the sum is not necessarily orthogonal.

Write $F : W \rightarrow U_1$ for the projector along U_2 . Show that $W = U_1^\perp \oplus U_2^\perp$ and F^\dagger projects W onto U_2^\perp along U_1^\perp .

Problem 19.4 (Harmonic Polynomials) Write U^* for the 3-dimensional real vector space with basis x, y, z and equip $SU^* \simeq \mathbb{R}[x, y, z]$ with a Euclidean inner product such that all monomials $x^\alpha y^\beta z^\gamma$ are mutually orthogonal with $(x^\alpha y^\beta z^\gamma, x^\alpha y^\beta z^\gamma) = \alpha! \beta! \gamma!$. Describe the adjoint operator of the Laplace operator $\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$ and show that the homogeneous degree- m polynomials can be decomposed as $S^m U^* = H_m \oplus \varrho^2 \cdot H_{m-2} \oplus \varrho^4 \cdot H_{m-4} \oplus \dots$, where $H_m = \{f \in S^m U^* \mid \Delta f = 0\}$ is the subspace of *harmonic* homogeneous degree- m polynomials and $\varrho^2 \stackrel{\text{def}}{=} x^2 + y^2 + z^2$.

²⁶See Sect. 10.2 on p. 233.

Problem 19.5 Let V be the space of smooth periodic functions $\mathbb{R} \rightarrow \mathbb{R}$ of period $T > 0$. Introduce a Euclidean scalar product on V by the prescription

$$(f, g) = \int_0^T f(x)g(x) dx.$$

Describe the adjoint operator to the linear differential operator of the form

$$a_k \frac{d^k}{dx^k} + a_{k-1} \frac{d^{k-1}}{dx^{k-1}} + \cdots + a_1 \frac{d}{dx} + a_0,$$

where $a_i = a_i(x) \in V$. Check whether the operator

$$\sin^2\left(\frac{2\pi x}{T}\right) \frac{d^2}{dx^2} + 2\pi T^{-1} \cos\left(\frac{4\pi x}{T}\right) \frac{d}{dx}$$

is self-adjoint.

Problem 19.6 Take $[a, b] = [0, 1]$ in Example 19.1 on p. 490 and check whether the operator

$$x^2(x-1)^2 \frac{d^2}{dx^2} + 2x(x-1) \frac{d}{dx}$$

is self-adjoint.

Problem 19.7 (Schur's Theorem) Prove that every \mathbb{C} -linear operator on a Hermitian space has an upper triangular matrix in some orthonormal basis.

Problem 19.8 Prove that for every normal operator F on a Hermitian space W :

- (a) Every two eigenvectors of F having different eigenvalues are orthogonal.
- (b) Every orthogonal collection of eigenvectors of F is included in some orthogonal basis of W formed by eigenvectors of F .

Problem 19.9 (Criteria of Normality 1) Prove that each of the following conditions on a \mathbb{C} -linear operator F on a Hermitian space is equivalent to the normality of F : (a) every eigenvector of F is an eigenvector for F^\dagger too, (b) $\|Fw\| = \|F^\dagger w\|$ for all w , (c) the orthogonal complement to every F -invariant subspace is F -invariant, (d) every F -invariant subspace is F^\dagger -invariant, (e) the self-adjoint and anti-self-adjoint parts of F commute, (f) the self-adjoint and unitary factors in the polar decomposition of F commute.

Problem 19.10 For every normal operator A and $k \in \mathbb{N}$, prove that the equation $X^k = A$ has a normal solution X . For which A can all solutions X be written as a polynomial in A ?

Problem 19.11 Prove that for every unitary operator U and $k \in \mathbb{N}$, the equation $X^k = U$ has a unitary solution X that may be written as a polynomial in U .

Problem 19.12 Let $F : \mathbb{C}^n \rightarrow \mathbb{C}^n$ be a self-adjoint operator with respect to the standard Hermitian structure.²⁷ For every r -dimensional subspace $L \subset \mathbb{C}^n$ with orthonormal basis e_1, e_2, \dots, e_r , put $R_L(F) \stackrel{\text{def}}{=} \sum_{i=1}^r (Fe_i, e_i)$. **(a)** Prove that $R_L(F)$ does not depend on the choice of orthonormal basis in L . **(b)** Assuming that F has distinct eigenvalues $\alpha_1 > \alpha_2 > \dots > \alpha_n$, find $\max_L R_L(F)$ over all r -dimensional subspaces $L \subset \mathbb{C}^n$.

Problem 19.13 (Courant–Fischer–Weyl Min–Max Principle) Let V be an n -dimensional Euclidean space and $Q : V \rightarrow V$ a self-adjoint operator with eigenvalues $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$. Write $q(v) = (v, Qv)$ for the quadratic form corresponding to Q . For every subspace $U \subset V$, let $m_U(q)$ and $M_U(q)$ denote the minimal and the maximal values of q on the unit sphere $\{u \in U : |u| = 1\}$ in U . Prove that $\max_{\dim U=k} m_U(q) = \alpha_k = \min_{\dim W=n+1-k} M_W(q)$.

Problem 19.14 Under the notation of [Problem 19.13](#), let $H \subset V$ be a hyperplane and $q|_H(v) = (v, Pv)$ for some self-adjoint operator on H with eigenvalues

$$\beta_1 \geq \beta_2 \geq \dots \geq \beta_{n-1}.$$

Show that $\alpha_1 \geq \beta_1 \geq \alpha_2 \geq \beta_2 \geq \dots \geq \alpha_{n-1} \geq \beta_{n-1} \geq \alpha_n$.

Problem 19.15 Show that the exponential map $K \mapsto e^K$ takes real skew-symmetric matrices to special orthogonal matrices. Is the resulting map

$$\text{End}_{\mathbb{R}}^-(\mathbb{R}^n) \rightarrow \text{SO}_n(\mathbb{R})$$

surjective?

Problem 19.16 (Cayley's Parametrization) Verify that the map

$$K \mapsto F = (E - K)(E + K)^{-1}$$

assigns a bijection between real skew-symmetric matrices K and real orthogonal matrices F such that $\text{Spec } F \not\ni -1$.

Problem 19.17 Prove that $\text{O}_n(\mathbb{R})$ and $\text{SO}_n(\mathbb{R})$ are compact subsets of $\text{Mat}_n(\mathbb{R})$. Are they path-connected?

Problem 19.18 An operator F on Euclidean space \mathbb{R}^3 with the standard inner product has matrix

$$\text{(a)} \begin{pmatrix} 1/2 & -\sqrt{3}/2 & 0 \\ \sqrt{3}/4 & 1/4 & -\sqrt{3}/2 \\ 3/4 & \sqrt{3}/4 & 1/2 \end{pmatrix}, \quad \text{(b)} \begin{pmatrix} \sqrt{2}/2 - \sqrt{2}/2 & 0 \\ 1/2 & 1/2 & -\sqrt{2}/2 \\ 1/2 & 1/2 & \sqrt{2}/2 \end{pmatrix},$$

²⁷See formula (18.14) on p. 470.

in the standard basis. Clarify whether F is a rotation or a rotation followed by a reflection in orthogonal plane to the rotation axis. In any case, find the axis and the angle of rotation.

Problem 19.19 Let V be a real Euclidean vector space. Show that the map $\text{End}(V) \rightarrow \text{Hom}(V, V^*)$ sending an operator $F : V \rightarrow V$ to the bilinear form $\beta_F(u, w) \stackrel{\text{def}}{=} (u, Fw)$ is an isomorphism of vector spaces that takes (anti)self-adjoint operators to (skew)symmetric forms. Deduce from this that every quadratic form on V can be written in some orthonormal basis of V as

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_rx_r^2.$$

Show that up to renumbering, the coefficients a_i do not depend on the choice of orthonormal basis.

Problem 19.20 Among the rectangular parallelepipeds circumscribed about the ellipsoid $x_1^2 + \frac{x_2^2}{4} + \frac{x_3^2}{9} = 1$ in the Euclidean space \mathbb{R}^3 , find the maximal and minimal lengths of their internal diagonals.

Problem 19.21 Find both Euclidean polar decompositions of the matrices (a) $\begin{pmatrix} 2 & -1 \\ 2 & 1 \end{pmatrix}$, (b) $\begin{pmatrix} 1 & 4 \\ 4 & 2 \end{pmatrix}$.

Problem 19.22 (Criteria of Normality 2) Prove all the criteria of normality from [Problem 19.9](#) for an \mathbb{R} -linear operator F on a Euclidean space.²⁸

Problem 19.23 Given a normal operator F on a real Euclidean space V , prove (independently of Theorem [19.1](#) on p. 491) that:

- (a) The orthogonal to every eigenspace of F is F -invariant.
- (b) The operators F, F^\vee are semisimple²⁹; moreover, V can be decomposed as an orthogonal direct sum of 1- and 2-dimensional subspaces invariant for both operators F and F^\vee .
- (c) For $\dim V = 2$ and irreducible F , the matrix of F in every orthonormal basis of V looks like

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \text{ where } b \neq 0.$$

- (d) Solve [Exercise 19.10](#) on p. 493 independently of Theorem [19.1](#) on p. 491.
- (e) Deduce Theorem [15.2](#) on p. 370 as well as Proposition [19.2](#) and Proposition [19.3](#) on p. 492 from [Exercise 19.10](#).

²⁸Of course, F^\dagger and $\|w\|$ should be replaced everywhere by F^\vee and $|w|$.

²⁹See Proposition [15.2](#) on p. 368.

Chapter 20

Quaternions and Spinors

20.1 Complex 2×2 Matrices and Quaternions

20.1.1 $\text{Mat}_2(\mathbb{C})$ as the Complexification of Euclidean \mathbb{R}^4

In Example 18.6 on p. 473, we saw that the complex structures on $V = \mathbb{R}^4$ that form the Hermitian plane \mathbb{C}^2 from Euclidean \mathbb{R}^4 are numbered by the lines on the Segre quadric¹ in $\mathbb{P}_3 = \mathbb{P}(\mathbb{C}^4)$. To see this correspondence in detail, let us identify the complexified space $W = V_{\mathbb{C}} = \mathbb{C}^4$ with the space of complex 2×2 matrices $\text{Mat}_2(\mathbb{C})$ in which the Segre quadric lives. The space $W = \text{Mat}_2(\mathbb{C})$ is equipped with a natural \mathbb{C} -bilinear form

$$\widetilde{\det} : W \times W \rightarrow \mathbb{C},$$

the polarization of the quadratic form \det , which is the equation of the Segre quadric. We would like to think of $\widetilde{\det}$ as the \mathbb{C} -bilinear extension of the Euclidean structure on V from V to $V_{\mathbb{C}} = \text{Mat}_2(\mathbb{C})$.

To write $\widetilde{\det}$ explicitly, recall² that for every matrix η , the formula $\eta \cdot \eta^{\vee} = \det \eta \cdot E$ holds, where η^{\vee} is the adjunct matrix³ of η . For 2×2 matrices, the map

$$\eta = \begin{pmatrix} \eta_{11} & \eta_{12} \\ \eta_{21} & \eta_{22} \end{pmatrix} \mapsto \eta^{\vee} \stackrel{\text{def}}{=} \begin{pmatrix} \eta_{22} & -\eta_{12} \\ -\eta_{21} & \eta_{11} \end{pmatrix} \quad (20.1)$$

¹See Example 17.6 on p. 439.

²See formula (9.29) on p. 221.

³See Sect. 9.6 on p. 220.

is a \mathbb{C} -linear involution. Therefore, the polarization of the determinant can be written as

$$\widetilde{\det}(\eta, \zeta) \stackrel{\text{def}}{=} \frac{1}{2} \operatorname{tr}(\eta \zeta^\vee). \quad (20.2)$$

Exercise 20.1 Verify that $\widetilde{\det}(\eta, \zeta)$ is symmetric and nondegenerate. Write its Gramian in the standard basis⁴ E_{ij} in Mat_2 . Check that the involution (20.1) is an antiautomorphism of the matrix algebra, meaning that $(\eta\zeta)^\vee = \zeta^\vee\eta^\vee$.

If we replace in (20.2) the adjunct matrix η^\vee by the Hermitian adjoint $\eta^\dagger = \overline{\eta}^t$, we get the \mathbb{C} -sesquilinear conjugate-symmetric form

$$(\eta, \zeta) \stackrel{\text{def}}{=} \frac{1}{2} \operatorname{tr}(\eta \zeta^\dagger) = \frac{1}{2} \sum_{i,j} \eta_{ij} \overline{\zeta}_{ij}, \quad (20.3)$$

which provides $\operatorname{Mat}_2(\mathbb{C})$ with a Hermitian structure such that the squared lengths of vectors equal

$$\|\eta\|^2 \stackrel{\text{def}}{=} (\eta, \eta) = \frac{1}{2} \sum |\eta_{ij}|^2,$$

and the standard basis E_{ij} is orthogonal with inner product squares $\|E_{ij}\|^2 = 1/2$. We would like to think of this Hermitian inner product as the \mathbb{C} -sesquilinear extension of the Euclidean structure on V from V to $V_{\mathbb{C}} = \operatorname{Mat}_2(\mathbb{C})$.

In fact, our two wishes uniquely determine the inclusion $V \hookrightarrow \operatorname{Mat}_2(\mathbb{C})$ as a real subspace of an appropriate real structure, because the \mathbb{C} -bilinear and \mathbb{C} -sesquilinear extensions of the same Euclidean inner product differ by complex conjugation of the second argument in the product. Therefore, a real structure

$$\sigma : \operatorname{Mat}_2(\mathbb{C}) \rightarrow \operatorname{Mat}_2(\mathbb{C})$$

that has V as a $+1$ -eigenspace should be the composition of the involution (20.1) with the Hermitian conjugation

$$\eta = \begin{pmatrix} \eta_{11} & \eta_{12} \\ \eta_{21} & \eta_{22} \end{pmatrix} \mapsto \eta^\dagger \stackrel{\text{def}}{=} \overline{\eta}^t = \begin{pmatrix} \overline{\eta}_{11} & \overline{\eta}_{21} \\ \overline{\eta}_{12} & \overline{\eta}_{22} \end{pmatrix}. \quad (20.4)$$

Exercise 20.2 Check that the involutions \vee and \dagger commute, and deduce from this that \vee, \dagger , their composition $\sigma = \vee \circ \dagger = \dagger \circ \vee$, and the identity map together form the Klein four group.⁵

⁴See Example 6.7 on p. 129.

⁵See Example 12.4 on p. 284.

Since Hermitian adjunction is a \mathbb{C} -antilinear matrix algebra antiautomorphism,⁶ its composition with (20.1) is a \mathbb{C} -antilinear matrix algebra automorphism:

$$\sigma : \eta = \begin{pmatrix} \eta_{11} & \eta_{12} \\ \eta_{21} & \eta_{22} \end{pmatrix} \mapsto \eta^\sigma \stackrel{\text{def}}{=} \begin{pmatrix} \bar{\eta}_{22} & -\bar{\eta}_{21} \\ -\bar{\eta}_{12} & \bar{\eta}_{11} \end{pmatrix}. \quad (20.5)$$

Exercise 20.3 Check by direct computation that $(\eta, \zeta) = \widetilde{\det}(\eta, \zeta^\sigma)$ and $(\eta\zeta)^\sigma = \eta^\sigma \zeta^\sigma$.

20.1.2 Algebra of Quaternions

A real subspace $V = \text{Re}_\sigma(W)$ with real structure (20.5) on $\text{Mat}_2(\mathbb{C})$ consists of matrices

$$x = \begin{pmatrix} x_1 + ix_2 & x_2 + ix_3 \\ -x_2 + ix_3 & x_1 - ix_2 \end{pmatrix}, \text{ where } x_\nu \in \mathbb{R}. \quad (20.6)$$

The restrictions of the \mathbb{R} -bilinear forms (20.2), (20.3) to V coincide and assign there the Euclidean structure $(x, x) = x_1^2 + x_2^2 + x_3^2 + x_4^2$, an orthonormal basis of which is formed, for example, by the matrices

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \stackrel{\text{def}}{=} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k \stackrel{\text{def}}{=} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}. \quad (20.7)$$

Since involution σ respects the multiplication, the fixed points of σ form an \mathbb{R} -subalgebra in $\text{Mat}_2(\mathbb{C})$. It is called the *algebra of quaternions* and is denoted by \mathbb{H} . The multiplication table of the basic quaternions (20.7) is

$$\begin{aligned} i^2 = j^2 = k^2 = -1, \\ ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j. \end{aligned} \quad (20.8)$$

Therefore, arbitrary quaternions are multiplied by the formula

$$\begin{aligned} (x_0 + x_1 i + x_2 j + x_3 k) \cdot (y_0 + y_1 i + y_2 j + y_3 k) = & (x_0 y_0 - x_1 y_1 - x_2 y_2 - x_3 y_3) \\ & + (x_0 y_1 + x_1 y_0 + x_2 y_3 - x_3 y_2) i + (x_0 y_2 + x_2 y_0 + x_3 y_1 - x_1 y_3) j \\ & + (x_0 y_3 + x_3 y_0 + x_1 y_2 - x_2 y_1) k, \end{aligned} \quad (20.9)$$

⁶That is, $(\eta\zeta)^\dagger = \zeta^\dagger \eta^\dagger$.

which is just a “command line utility” for matrix multiplication of special matrices (20.6).

Exercise 20.4 Given an abstract real vector space \mathbb{R}^4 with the basis $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ satisfying the multiplication table (20.8), try to verify that formula (20.9) provides this space \mathbb{R}^4 with the structure of an associative \mathbb{R} -algebra.

20.1.3 Real and Pure Imaginary Quaternions

By analogy with the complex numbers, the quaternions of the real line spanned by the unit $\mathbb{R} \cdot 1 \subset \mathbb{H}$ are called *real*, whereas the quaternions lying in the 3-dimensional subspace $I \stackrel{\text{def}}{=} \{x \cdot \mathbf{i} + y \cdot \mathbf{j} + z \cdot \mathbf{k} \mid x, y, z \in \mathbb{R}\}$ are called *pure imaginary*. In the language of matrices, the pure imaginary quaternions are exactly the anti-Hermitian traceless matrices: $I = \{\eta \in \text{Mat}_2(\mathbb{C}) \mid \eta^\dagger = -\eta, \text{tr } \eta = 0\}$. The real quaternions are the real scalar matrices $\mathbb{R} \cdot E$. Thus, Hermitian adjunction of matrices fixes all real quaternions and changes signs of all pure imaginary quaternions. In analogy with complex numbers, this operation is called *quaternionic conjugation* and traditionally is denoted by an asterisk:

$$qx_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k} \mapsto q^* \stackrel{\text{def}}{=} q^\dagger = x_0 - x_1\mathbf{i} - x_2\mathbf{j} - x_3\mathbf{k}.$$

This is an antiautomorphism of the \mathbb{R} -algebra \mathbb{H} , i.e., $(pq)^* = q^*p^*$. Note also that the real and imaginary quaternions are orthogonal in the Euclidean structure on \mathbb{H} . Indeed, formula (20.9) shows that the Euclidean scalar product is related to the multiplication by the equalities

$$(p, q) = \text{Re}(pq^*) = \text{Re}(p^*q), \quad (20.10)$$

which force $(1, \mathbf{i}) = (1, \mathbf{j}) = (1, \mathbf{k}) = 0$.

20.1.4 Quaternionic Norm

Since the squared Euclidean length of a quaternion $\eta = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$ is nothing but the determinant, $\|\eta\|^2 = \sum x_v^2 = (\eta, \eta) = \det(\eta)$, the Euclidean length is multiplicative with respect to quaternionic multiplication: $\|\eta\zeta\| = \|\eta\| \cdot \|\zeta\|$ for all $\eta, \zeta \in \mathbb{H}$. Traditionally, the length of a quaternion is called the *quaternionic norm*. The multiplicativity of the norm can also be seen directly from the relations (20.8) as follows. For every $q \in \mathbb{H}$, the product $q \cdot q^*$ is self-adjoint and therefore real, that is, $q \cdot q^* = \text{Re}(q \cdot q^*)$. So, formula (20.10) written for $p = q$ becomes the remarkable

equality

$$\|q\|^2 = qq^*, \quad (20.11)$$

similar to what we have for the complex numbers. The multiplicativity of the norm now follows:

$$\|pq\|^2 = pq(pq)^* = pqq^*p^* = p\|q\|^2p^* = \|p\|^2\|q\|^2.$$

It is quite astonishing that the coordinate form of this relation, called *Euler's four-square identity*,

$$\begin{aligned} & (x_0^2 + x_1^2 + x_2^2 + x_3^2) \cdot (y_0^2 + y_1^2 + y_2^2 + y_3^2) \\ &= (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3)^2 + (x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2)^2 \\ & \quad + (x_0y_2 + x_2y_0 + x_3y_1 - x_1y_3)^2 + (x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1)^2, \end{aligned} \quad (20.12)$$

appeared in 1748, in a letter from Euler to Christian Goldbach, almost a century before the multiplication table (20.8) was discovered by Sir William Rowan Hamilton in 1843. (Euler's four-square identity was used by Joseph Louis Lagrange in 1770 to prove that every nonnegative integer can be represented as the sum of four perfect squares.)

20.1.5 Division

Another crucial consequence of (20.11) is the invertibility of every nonzero quaternion $q \in \mathbb{H}$. Namely, a quaternion $q^{-1} = q^*/\|q\|^2$ is clearly a two-sided inverse to q . Thus, \mathbb{H} is an associative, noncommutative *division algebra*⁷ over the field \mathbb{R} , meaning that the addition and multiplication of quaternions satisfy all the field axioms except for the commutativity of multiplication.

20.2 Geometry of Quaternions

Recall that the *cross product* of two vectors u, w in the Euclidean space \mathbb{R}^3 equipped with the standard orientation is a vector $u \times w \in \mathbb{R}^3$ uniquely determined by the following properties:

⁷Or *skew field*.

- The length $|u \times w|$ equals the Euclidean area of the parallelogram spanned by u, w .
- If $u \times w \neq 0$, then $u, w, u \times w$ is an orthogonal basis of positive orientation.

Equivalently, we could say that $u \times w \in V$ is the Euclidean dual vector to the covector

$$\omega(u, w, *) : V \rightarrow \mathbb{R}, \quad v \mapsto \omega(u, w, v),$$

where ω is the standard volume form on \mathbb{R}^3 assigning the unit volume to the standard basis.

Exercise 20.5 Convince yourself of the equivalence of both definitions. Then for two vectors $u = (u_1, u_2, u_3)$, $w = (w_1, w_2, w_3)$, write the orthogonality relations

$$\begin{cases} (u, x) = u_1x_1 + u_2x_2 + u_3x_3 = 0, \\ (w, x) = w_1x_1 + w_2x_2 + w_3x_3 = 0, \end{cases}$$

in the unknown vector $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ and verify that the basic solution of these equations provided by Cramer's rule from Proposition 9.5 on p. 224 coincides with the cross product:

$$x = (u_2w_3 - w_2u_3, -u_1w_3 + w_1u_3, u_1w_2 - w_1u_2) = u \times w.$$

Lemma 20.1 Take $\mathbf{i}, \mathbf{j}, \mathbf{k}$ from (20.7) as the standard orienting basis in the Euclidean space of pure imaginary quaternions $I \simeq \mathbb{R}^3$. Then $\text{Im}(pq) = p \times q$ for all $p, q \in I$. In particular, pq is real if and only if $q = \lambda p$ for some $\lambda \in \mathbb{R}$.

Proof Since both maps $p, q \mapsto p \times q$ and $p, q \mapsto \text{Im}(pq)$ are bilinear, it is enough to check the relation $\text{Im}(pq) = p \times q$ for nine pairs of basic vectors $p, q = \mathbf{i}, \mathbf{j}, \mathbf{k}$. This is exactly the multiplication table (20.8). \square

Lemma 20.2 Two arbitrary quaternions $p, q \in \mathbb{H}$ are orthogonal if and only if $pq^* \in I$. Two pure imaginary quaternions $p, q \in I$ are orthogonal if and only if $pq = -qp$, and in this case, $pq = -qp \in I$ is perpendicular to the plane spanned by p, q .

Proof The first statement follows directly from formula (20.10). All other claims follow from Lemma 20.1. \square

Lemma 20.3 The solution set of the equation $x^2 = -1$ in \mathbb{H} is the unit sphere $S^2 = \{x \in I \mid \|x\| = 1\}$ in $I \simeq \mathbb{R}^3$.

Proof The equation $x^2 = -1$ forces $\|x\| = 1$. Then $x^* = x^{-1} = -x$, and therefore $x \in I$. Conversely, for every $x \in S^2$, we have $x^2 = -x^*x = -x^{-1}x = -1$. \square

Lemma 20.4 Three arbitrary quaternions $\mathbf{i}, \mathbf{j}, \mathbf{k}$ satisfy the relations (20.8) if and only if they form a positive orthonormal basis in I , where the orientation in I is given by the initial orthonormal basis (20.7).

Proof The relations $i^2 = j^2 = k^2 = -1$ mean that all three quaternions lie on the unit sphere $S^2 \subset I$. Then by Lemma 20.2, the relations $i \cdot j = k = -j \cdot i$ mean that k is perpendicular to both i and j , and the orthonormal basis i, j, k is positive. \square

20.2.1 Universal Covering $S^3 = \text{SU}_2 \twoheadrightarrow \text{SO}_3(\mathbb{R})$

For matrices of determinant 1, the adjunct matrix coincides with the inverse. Hence the special unitary group

$$\text{SU}_2 = \{\eta \in \text{Mat}_2(\mathbb{C}) \mid \det \eta = 1 \text{ \& } \eta^{-1} = \eta^\dagger\}$$

consists of all $\eta \in \text{Mat}_2(\mathbb{C})$ with $\det \eta = 1$ and $\eta^\vee = \eta^\dagger$. The latter means that η is σ -real and therefore lies in \mathbb{H} . We conclude that SU_2 coincides with the unit sphere

$$S^3 = \{\psi \in \mathbb{H} \mid \|\psi\| = 1\} \subset \mathbb{H} \simeq \mathbb{R}^4.$$

This group acts on the quaternionic algebra \mathbb{H} by conjugation. Namely, for every $\psi \in S^3$, let⁸

$$F_\psi : \mathbb{H} \rightarrow \mathbb{H}, \quad q \mapsto \psi q \psi^{-1}. \quad (20.13)$$

Exercise 20.6 Check that F_ψ is an \mathbb{R} -algebra automorphism and

$$F : \text{SU}_2 \rightarrow \text{Aut}(\mathbb{H}), \quad \psi \mapsto F_\psi,$$

is a group homomorphism.

Since $\det(\psi q \psi^{-1}) = \det q$, the operator F_ψ is a Euclidean isometry of \mathbb{H} . Since F_ψ preserves the central line $\mathbb{R} \cdot 1$, the space $I = 1^\perp$ of pure imaginary quaternions is F_ψ -invariant. As ψ is continuously deformed to 1 within S^3 , the restricted orthogonal isometry $F_\psi|_I : I \simeq I$ is continuously deformed to Id_I within $\text{O}_{\det}(I)$. Therefore, $F_\psi \in \text{SO}_{\det}(I) \simeq \text{SO}_3(\mathbb{R})$. We get the group homomorphism

$$S^3 = \text{SU}_2 \rightarrow \text{SO}_{\det}(I) \simeq \text{SO}_3(\mathbb{R}), \quad \psi \mapsto F_\psi|_I. \quad (20.14)$$

Since $F_\psi(\psi) = \psi$ and $F_\psi(1) = 1$, the operator $F_\psi : \mathbb{H} \rightarrow \mathbb{H}$ leaves fixed each vector in the 2-dimensional plane $\Pi_\psi = \mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot \psi$. Therefore, $F_\psi|_I : I \rightarrow I$ is a rotation about the line $\ell_\psi \stackrel{\text{def}}{=} \Pi_\psi \cap I$. Let us fix one of two pure imaginary quaternions

⁸Since $\psi^{-1} = \psi^*$ for every ψ with $\|\psi\| = 1$, the same operator could be described by the formula $F_\psi : q \mapsto \psi q \psi^*$.

of length 1 on this line⁹ and denote it by \mathbf{l} . We identify the real plane Π_ψ with the field \mathbb{C} by

$$\mathbb{C} \ni (x + iy) \longleftrightarrow (x + y\mathbf{l}) \in \Pi_\psi. \quad (20.15)$$

Such an identification provides our quaternion $\psi \in \Pi_\psi \simeq \mathbb{C}$ with an *argument* $\alpha = \text{Arg } \psi$ uniquely determined by the equality $\psi = \cos \alpha + \mathbf{l} \cdot \sin \alpha$. Therefore, $\psi^{-1} = \cos \alpha - \mathbf{l} \cdot \sin \alpha$.

Lemma 20.5 *The operator $F_\psi|_I \in \text{SO}_{\det}(I)$ is rotation about the line ℓ_ψ by the angle $2 \text{Arg}(\psi)$ viewed in the direction of the vector $\mathbf{l} \in \ell_\psi$.*

Proof Fit the vector \mathbf{l} into the positively oriented orthonormal basis $\mathbf{l}, \mathbf{m}, \mathbf{n}$ in I . By Lemma 20.4, the multiplication table of quaternions $\mathbf{l}, \mathbf{m}, \mathbf{n}$ is $\mathbf{l}^2 = \mathbf{m}^2 = \mathbf{n}^2 = \mathbf{l}\mathbf{m}\mathbf{n} = -1$ as in (20.8). Therefore,

$$\begin{aligned} \psi \mathbf{m} \psi^{-1} &= (\cos \alpha + \mathbf{l} \cdot \sin \alpha) \mathbf{m} (\cos \alpha - \mathbf{l} \cdot \sin \alpha) \\ &= (\mathbf{m} \cos \alpha + \mathbf{n} \cdot \sin \alpha) (\cos \alpha - \mathbf{l} \cdot \sin \alpha) \\ &= \mathbf{m} (\cos^2 \alpha - \sin^2 \alpha) + 2\mathbf{n} \cos \alpha \sin \alpha = \mathbf{m} \cos(2\alpha) + \mathbf{n} \sin(2\alpha), \\ \psi \mathbf{n} \psi^{-1} &= (\cos \alpha + \mathbf{l} \cdot \sin \alpha) \mathbf{n} (\cos \alpha - \mathbf{l} \cdot \sin \alpha) \\ &= (\mathbf{n} \cos \alpha - \mathbf{m} \cdot \sin \alpha) (\cos \alpha - \mathbf{l} \cdot \sin \alpha) \\ &= \mathbf{n} (\cos^2 \alpha - \sin^2 \alpha) - 2\mathbf{m} \cos \alpha \sin \alpha = \mathbf{n} \cos(2\alpha) - \mathbf{m} \sin(2\alpha). \end{aligned}$$

Thus, F_ψ acts on the vectors (\mathbf{m}, \mathbf{n}) by the matrix $\begin{pmatrix} \cos(2\alpha) & -\sin(2\alpha) \\ \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$. \square

Corollary 20.1 *The group homomorphism (20.14) is surjective with kernel $\{\pm 1\} \simeq \mathbb{Z}/(2)$.* \square

20.2.2 Topological Comment

In topological language, the homomorphism (20.14) is a double covering of $\text{SO}_3(\mathbb{R})$ by the sphere S^3 . Since the map (20.14) identifies the diametrically opposite points of the sphere, its image is homeomorphic to the real projective space $\mathbb{P}_3 = \mathbb{P}(\mathbb{H})$. Hence, $\text{SO}_3(\mathbb{R})$ is homeomorphic to $\mathbb{P}(\mathbb{R}^4)$. Since the sphere S^3 is simply connected¹⁰ and the group $\text{SO}_3(\mathbb{R})$ is path-connected, the covering (20.14) is a *universal covering*. This means, in particular, that $\pi_1(\text{SO}_3) = \mathbb{Z}/(2)$, i.e., there

⁹These two quaternions are the intersection points $\ell_\psi \cap S^2$ and are opposites of each other.

¹⁰That is, the fundamental group $\pi_1(S^3)$ is trivial.

is a smooth noncontractible loop within $SO_3(\mathbb{R})$ that becomes contractible after being traversed twice. Such a loop, that is, a rotation, which varies depending on time and becomes the identity after some time, can be visualized as follows. Put a book in the palm of your hand and rotate it slowly through 360° keeping it horizontal all the time, as in Fig. 20.1, which is borrowed from a remarkable book by George K. Francis.¹¹ After a full turn, your hand becomes exactly that loop in SO_3 . A troublesome tension in your elbow joint distinctly witnesses against the contractibility of this loop. However, if you overcome the discomfort and continue to rotate the book *in the same direction*, then during the next turn, your hand straightens itself and returns to the starting “contracted” position.

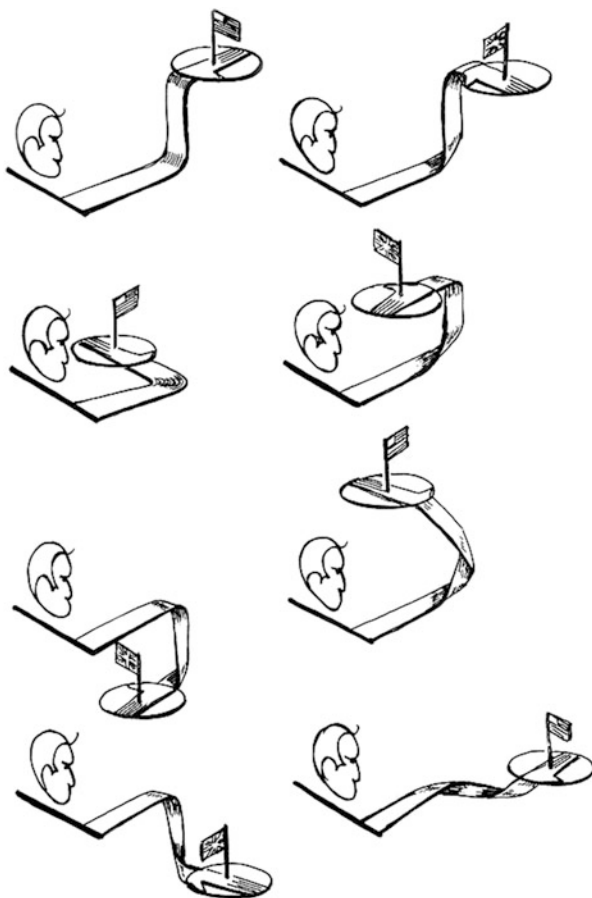


Fig. 20.1 Rotating a book

¹¹A *Topological Picturebook* [Fr].

20.2.3 Two Pencils of Hermitian Structures

By Lemma 20.3, every pure imaginary quaternion \mathbf{n} of norm 1 has $\mathbf{n}^2 = -1$. Therefore, left and right multiplication by such quaternions provides $\mathbb{H} = \mathbb{R}^4$ with two families of complex structures:

$$I'_n : \mathbb{H} \rightarrow \mathbb{H}, \quad \eta \mapsto \mathbf{n}\eta, \quad \text{and} \quad I''_n : \mathbb{H} \rightarrow \mathbb{H}, \quad \eta \mapsto \eta\mathbf{n}, \quad (20.16)$$

compatible with the Euclidean structure¹² on \mathbb{H} and numbered by the points $\mathbf{n} \in S^2$ on the unit sphere in $I \simeq \mathbb{R}^3$. The real plane $\Pi_n = \mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot \mathbf{n}$ is invariant with respect to both operators (20.16) and can be identified with the field \mathbb{C} by the same rule $x + iy \leftrightarrow x + y\mathbf{n}$ as in formula (20.15) above. Choose some $\mathbf{m} \in S^2 \cap \Pi_n^\perp$. Then \mathbb{H} , considered a 2-dimensional vector space over \mathbb{C} , can be decomposed into the direct sum of two 1-dimensional subspaces¹³

$$\mathbb{C} \cdot 1 \oplus \mathbb{C} \cdot \mathbf{m} = \mathbb{H} = 1 \cdot \mathbb{C} \oplus \mathbf{m} \cdot \mathbb{C}. \quad (20.17)$$

Multiplication by the complex number $i \in \mathbb{C}$ acts on left and right decomposition respectively as left and right multiplication by \mathbf{n} . These actions coincide on $\mathbb{C} \cdot 1 = \Pi_n = 1 \cdot \mathbb{C}$ and are conjugate to each other on $\mathbb{C} \cdot \mathbf{m} = \Pi_n^\perp = \mathbf{m} \cdot \mathbb{C}$, because $I'_n(\mathbf{m}) = \mathbf{n}\mathbf{m} = -\mathbf{m}\mathbf{n} = -I''_n(\mathbf{m})$. Therefore, the two complex structures (20.16) are distinct. Clearly, each of them differs from all structures I'_l, I''_l with $l \neq \pm\mathbf{n}$, because the latter do not send the plane Π_n to itself. The operators I'_n and $I'_{-\mathbf{n}} = -I'_n$ provide the real plane $\Pi_n = \Pi_{-\mathbf{n}}$ with conjugate complex structures and therefore are distinct as well. The same holds for the operators I''_n and $I''_{-\mathbf{n}} = -I''_n$ as well as for the operators I'_n and $I''_{-\mathbf{n}}$. Thus, we see that all complex structures (20.16) are in fact distinct.

Note that this agrees with Example 18.6 on p. 473, because both line rulings of the Segre quadric are parametrized by $\mathbb{P}_1(\mathbb{C}) \simeq S^2$ (see Fig. 11.4 in Example 11.1 on p. 256).

Exercise 20.7 Convince yourself that the decomposition (20.17) is much like the presentation of the complex number field in the form $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$. Namely, one could *define* \mathbb{H} as a “double \mathbb{C} ,” that is, a set of formal records $z + w \cdot \mathbf{j}$, where $z, w \in \mathbb{C}$ and the symbol \mathbf{j} has $\mathbf{j}^2 = -1$ and is \mathbb{C} antilinear: $\mathbf{j}z = \overline{\mathbf{j}}\overline{z}$. In other words, the records are multiplied according to the rule

$$(z_1 + w_1 \cdot \mathbf{j}) \cdot (z_2 + w_2 \cdot \mathbf{j}) \stackrel{\text{def}}{=} (z_1 z_2 - w_1 \overline{w_2}) + (z_1 w_2 + w_1 \overline{z_2}) \cdot \mathbf{j}.$$

¹²In the sense of Proposition 18.4 on p. 472; essentially this means that the Euclidean length of a vector coincides with its Hermitian norm.

¹³The left decomposition is valid in the complex structure I'_n , whereas the right holds for I''_n .

20.3 Spinors

20.3.1 Geometry of Hermitian Enhancements of Euclidean \mathbb{R}^4

Let us return to the notation from Example 17.6 on p. 439, that is, we shall consider a 2-dimensional Hermitian vector space $U = \mathbb{C}^2$ and put $W = \text{End}_{\mathbb{C}}(U)$. This W again becomes $\text{Mat}_2(\mathbb{C})$ as soon as we fix some orthonormal basis in U and write all the operators $\eta : U \rightarrow U$ in this basis using matrices. The points on the two dual projective lines $\mathbb{P}_1^{\times} = \mathbb{P}(U^*)$ and $\mathbb{P}_1 = \mathbb{P}(U)$ are called *spinors*.¹⁴ They are in bijection with the complex structures (20.16) on \mathbb{H} as follows. The Segre embedding¹⁵

$$\begin{aligned} \mathbb{P}_1^{\times} \times \mathbb{P}_1 &\simeq Z(\det) \subset \mathbb{P}(W), & (\xi, v) &\mapsto \xi \otimes v \in \text{End}(U), \\ \text{where } \xi \otimes v : U &\rightarrow U, & u &\mapsto \xi(u) \cdot v, \end{aligned} \quad (20.18)$$

sends the coordinate lines $\xi \times \mathbb{P}_1$ and $\mathbb{P}_1^{\times} \times v$ to the lines on the Segre quadric $Z(\det) \subset \mathbb{P}(W)$. The latter lines are projectivizations of the 2-dimensional subspaces

$$U_{\xi} = \{F : U \rightarrow U \mid \ker F = \text{Ann } \xi\} \quad \text{and} \quad U_v = \{F : U \rightarrow U \mid \text{im } F = \mathbb{C} \cdot v\}$$

in W . Write $I_v : V \rightarrow V$ for the complex structure provided by U_v in accordance with Proposition 18.4 on p. 472 and let $I_v^{\mathbb{C}} : W \rightarrow W$ denote the complexified operator. Then the $+i$ and $-i$ eigenspaces of $I_v^{\mathbb{C}}$ are U_v and $\sigma(U_v)$, where

$$\sigma : W \rightarrow W$$

is the real structure defined in formula (20.5) on p. 505. The Segre quadric has no σ -real points, because the restriction of the quadratic form $\det : W \rightarrow \mathbb{C}$ to V is a positive Euclidean form. Therefore, σ sends every line on $Z(\det)$ to a line from the same ruling family.¹⁶ In other words, σ acts on the spinor lines $\mathbb{P}_1^{\times}, \mathbb{P}_1$, and the σ -conjugate subspaces $U_v, \sigma(U_v) = U_{\sigma(v)}$ come from some σ -conjugate spinors $v, \sigma(v)$. Since U_v and $U_{\sigma(v)}$ consist of rank-1 operators $F : U \rightarrow U$ whose images are spanned by v and $\sigma(v)$, the operator $I_v^{\mathbb{C}} : W \rightarrow W$ is forced to be left multiplication by the operator

$$\psi_v : U \rightarrow U, \quad \begin{cases} v \mapsto iv, \\ \sigma(v) \mapsto -i\sigma(v) = \sigma(iv). \end{cases} \quad (20.19)$$

By construction, this operator is σ -invariant, i.e., lies in $V = \mathbb{H}$. We conclude that the complex structure $I_v : \mathbb{H} \rightarrow \mathbb{H}$ acts as left multiplication by the quaternion $\psi_v \in \mathbb{H}$ defined in formula (20.19). This quaternion is also called a *spinor*.

¹⁴Physicists like to say that these two families of dual spinors are of *opposite chiralities*.

¹⁵See 17.13 on p. 439.

¹⁶If the lines ℓ and $\sigma(\ell)$ lie in different families, then their intersection $\ell \cap \sigma(\ell)$ is a real point of $Z(\det)$.

Symmetrically, write $\sigma^* : U^* \rightarrow U^*$ for the dual action of σ on U^* . Then the det-isotropic subspaces U_ξ and $\sigma(U_\xi) = U_{\sigma^*(\xi)}$ come from some σ^* -conjugate spinors ξ and $\sigma^*(\xi) = \xi \circ \sigma$. They consist of rank-1 operators $F : U \rightarrow U$ taking $u \in U$ respectively to $\xi(u) \cdot w'$ and to $\xi(\sigma u) \cdot w''$ for some $w', w'' \in W$. Therefore, $I_v^{\mathbb{C}}$ sends $F : U \rightarrow U$ to $F \circ \psi_\xi$, where $\psi_\xi : U \rightarrow U$ satisfies the conditions

$$\psi_\xi^* : U^* \rightarrow U^*, \quad \begin{cases} \xi \mapsto i\xi, \\ \xi \circ \sigma \mapsto -i\xi \circ \sigma = \xi \circ (i\sigma). \end{cases} \quad (20.20)$$

By construction, $\psi_\xi \in \mathbb{H}$ and the complex structure $I_\xi : \mathbb{H} \rightarrow \mathbb{H}$ acts as right multiplication by ψ_ξ . The quaternion ψ_ξ is called a *spinor*¹⁷ as well.

20.3.2 Explicit Formulas

Fix a standard basis in $U = \mathbb{C}^2$ and write the vectors $v \in U$ as coordinate columns and covectors $\xi \in U^*$ and coordinate rows. The spinor space U is equipped with a \mathbb{C} -linear skew-symmetric correlation $\delta : U \rightarrow U^*$, $\delta^* = -\delta$, provided by the nondegenerate skew-symmetric form¹⁸ \det . It takes a vector $v \in U$ to the covector

$$\delta v : u \mapsto \det(u, v) = u_0 v_1 - u_1 v_0, \quad \text{i.e., } \delta : \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \mapsto (v_1, -v_0).$$

The involution $F \mapsto F^\vee = \delta^{-1} F^* \delta$ on $W = \text{End}(U)$ is the (right) adjunction of operators¹⁹ by the correlation δ . Also, there is a \mathbb{C} -antilinear correlation $h : U \rightarrow U^*$ provided by the Hermitian inner product $(*, *)_{\mathbb{H}}$ on U . It takes a vector $v \in U$ to the covector $h v : u \mapsto (u, v)_{\mathbb{H}} = u_0 \bar{v}_0 + u_1 \bar{v}_1$, i.e.,

$$h : \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \mapsto (\bar{v}_0, \bar{v}_1).$$

The involution $F \mapsto F^\dagger = h^{-1} F^* h$ on W takes F to the Hermitian adjoint operator with respect to h . The real structure $\sigma = \vee \circ \dagger$ on W maps $F \mapsto F^\sigma = F^{\vee \dagger} = h^{-1} \delta^* F \delta^{*-1} h = (\delta^{-1} h)^{-1} F \delta^{-1} h$, i.e., conjugates endomorphisms of U by the \mathbb{C} -antilinear involution

$$\sigma_U = \delta^{-1} h : U \rightarrow U, \quad \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \mapsto \begin{pmatrix} -\bar{v}_1 \\ \bar{v}_0 \end{pmatrix}.$$

¹⁷Of chirality other than ψ_v .

¹⁸See Example 6.4 on p. 125.

¹⁹See Sect. 16.3, especially formula (16.24) on p. 399.

Note that it has no fixed points on $\mathbb{P}_1 = \mathbb{P}(U)$. To find the matrix ψ_v that corresponds to the spinor $v = (z_0 : z_1) \in \mathbb{P}_1$, let us normalize $v \in U$ by the condition²⁰ $(v, v)_H = z_0 \bar{z}_0 + z_1 \bar{z}_1 = 1$. Then

$$\det \begin{pmatrix} z_0 & -\bar{z}_1 \\ z_1 & \bar{z}_0 \end{pmatrix} = 1 \quad (20.21)$$

as well. The operator ψ_v has a diagonal matrix with eigenvalues $+i, -i$ in the basis $v, \sigma v$. Therefore, in the standard basis of $U = \mathbb{C}^2$, the matrix of ψ_v is equal to

$$\begin{pmatrix} z_0 & -\bar{z}_1 \\ z_1 & \bar{z}_0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} z_0 & -\bar{z}_1 \\ z_1 & \bar{z}_0 \end{pmatrix}^{-1} = i \cdot \begin{pmatrix} |z_0|^2 - |z_1|^2 & 2z_0 \bar{z}_1 \\ 2\bar{z}_0 z_1 & |z_1|^2 - |z_0|^2 \end{pmatrix}.$$

Thus, the complex structure $I_v : \mathbb{H} \rightarrow \mathbb{H}$ corresponding to the spinor

$$v = (z_0 : z_1) \in \mathbb{P}_1$$

acts as left multiplication by the pure imaginary quaternion

$$\psi_v = (|z_0|^2 - |z_1|^2) \cdot \mathbf{i} + 2z_0 \bar{z}_1 \cdot \mathbf{k}. \quad (20.22)$$

Exercise 20.8 Check that $\|\psi_v\| = 1$ and verify that the complex structure I_ξ provided by the spinor $\xi = \delta v = (-z_1 : z_0) \in \mathbb{P}_1^\times$ acts on \mathbb{H} as right multiplication by ψ_v .

20.3.3 Hopf Bundle

The correspondence $v \mapsto \psi_v$ described above in fact maps the 3-sphere

$$S^3 = \{v \in U \mid (v, v)_H = 1\} \subset \mathbb{C}^2 \simeq \mathbb{R}^4$$

onto the 2-sphere of pure imaginary quaternions of norm 1:

$$S^2 = \{q \in I \mid \|q\| = 1\} \subset I \simeq \mathbb{R}^3.$$

The quaternion ψ_v in (20.22) does not depend on the *phase* of the spinor v , i.e., it is not changed under rescaling $v \mapsto \vartheta v$ by $\vartheta \in U_1 = S^1 \subset \mathbb{C}$. Thus, the fibers of the map

$$S^3 \twoheadrightarrow S^2, \quad v \mapsto \psi_v, \quad (20.23)$$

²⁰This can be done via multiplication of v by an appropriate positive real constant.

are unit circles within S^3 . The map (20.23) is called the *Hopf bundle*. In purely topological terms, it is described as follows. The complex projective line $\mathbb{P}(\mathbb{C}^2) = \mathbb{P}_1 \simeq S^2$ is the space of nonzero orbits for the action of the multiplicative group \mathbb{C}^* on \mathbb{C}^2 by scalar dilatations. Since $\mathbb{C}^* = \mathbb{R}_{>0}^* \times U_1$, the quotient map $\mathbb{C}^2 \setminus 0 \rightarrow \mathbb{P}_1$ can be factored into the composition of the quotient map

$$\mathbb{C}^2 \setminus 0 \rightarrow \mathbb{C}^2 \setminus 0 / \mathbb{R}_{>0}^* \simeq S^3$$

followed by the quotient map $S^3 \rightarrow S^2 = S^3 \setminus 0 / U_1$. The first takes a nonzero vector $u \in \mathbb{C}^2$ to the unique $v = \lambda u$ with $\lambda \in \mathbb{R}_{>0}$ such that $(v, v)_H = 1$. This is exactly the normalization made in formula (20.21) above. The second quotient map, which factorizes the unit sphere by phase shifts, is the Hopf bundle.

Problems for Independent Solution to Chap. 20

Problem 20.1 Give a basis in $\text{Mat}_2(\mathbb{C})$ in which the Gramian of the quadratic form \det is diagonal with diagonal elements $(+1, -1, -1, -1)$.

Problem 20.2 For $q \in \mathbb{H}$, let $C(q) = \{w \in \mathbb{H} \mid wq = qw\}$. For all possible values of $\dim_{\mathbb{R}} C(q)$, describe all quaternions $q \in \mathbb{H}$ with that value. In particular, show that the center $Z(\mathbb{H})$ is equal to $\mathbb{R} \cdot 1$.

Problem 20.3 Show that every nonreal quaternion is a root of a quadratic polynomial with real coefficients and negative discriminant.

Problem 20.4 Solve the following systems of linear equations in $x, y \in \mathbb{H}$:

$$\text{(a)} \begin{cases} k = (i + j) \cdot x + (1 + k) \cdot y, \\ i = (1 + i) \cdot x + (j + k) \cdot y, \end{cases} \quad \text{(b)} \begin{cases} k = (1 + i) \cdot x + j \cdot y, \\ i = (1 + j) \cdot x + k \cdot y. \end{cases}$$

Problem 20.5 Check that the subspaces

$$\{q \in \mathbb{H} \mid q^* = -q\} \text{ and } \{q \in \mathbb{H} \mid q^2 \in \mathbb{R}_{\leq 0} \cdot 1\}$$

coincide. Denote them by $I \subset \mathbb{H}$. Show that

- (a) the map $x, y \mapsto [x, y] \stackrel{\text{def}}{=} xy - yx$ sends $I \times I$ to I ,
- (b) the \mathbb{R} -bilinear form $(p, q) \stackrel{\text{def}}{=} (pq^* + qp^*)/2$ provides I with a Euclidean structure,
- (c) this Euclidean structure coincides with $\widetilde{\det}|_I$,
- (d) $[x, y] = x \times y$ for all $x, y \in I$.

Problem 20.6 For every nonzero $\alpha \in \mathbb{H}$, show that the conjugation map

$$\varphi_\alpha : \mathbb{H} \rightarrow \mathbb{H}, q \mapsto \alpha q \alpha^{-1},$$

is an automorphism of the \mathbb{R} -algebra \mathbb{H} and a Euclidean isometry of the subspace of pure imaginary quaternions $I \subset \mathbb{H}$.

Problem 20.7 For a given complex 2×2 matrix $\alpha \in \mathrm{SU}_2 \subset \mathbb{H}$, write down an explicit real 3×3 matrix of the orthogonal operator $\varphi_\alpha : I \rightarrow I$ from [Problem 20.6](#) in the basis i, j, k .

Problem 20.8 For two matrices $g_1, g_2 \in \mathrm{SL}_2(\mathbb{C})$, write $\psi_{g_1, g_2} \in \mathrm{End}_{\mathbb{C}}(\mathrm{Mat}_2(\mathbb{C}))$ for the linear endomorphism $X \mapsto g_1 X g_2^{-1}$. Check that the assignment

$$(g_1, g_2) \mapsto \psi_{g_1, g_2}$$

yields a well-defined group homomorphism

$$\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C}) \rightarrow \mathrm{SO}_{\det}(\mathrm{Mat}_2(\mathbb{C})).$$

Describe its kernel and its image. For given matrices $g_1, g_2 \in \mathrm{SL}_2(\mathbb{C})$, write down an explicit real orthogonal 4×4 matrix of the operator ψ_{g_1, g_2} in the basis you have constructed in [Problem 20.1](#).

Problem 20.9 For two quaternions $p, q \in \mathbb{H}$ of unit norm $\|\varphi\| = \|\psi\| = 1$, write $\psi_{pq} : \mathbb{H} \rightarrow \mathbb{H}$ for the linear endomorphism $\eta \mapsto p\eta q^{-1}$. Check that the map $(p, q) \mapsto \psi_{p, q}$ is a well-defined group epimorphism $\mathrm{U}_2 \times \mathrm{U}_2 \rightarrow \mathrm{SO}_4(\mathbb{R})$. Describe its kernel. For given quaternions p, q , write down an explicit real orthogonal 4×4 matrix of the operator ψ_{pq} in the basis $1, i, j, k$.

Problem 20.10 Write $e \in \mathbb{H}$ for the unit of the quaternionic algebra. Prove that the following collections of quaternions form multiplicative subgroups in \mathbb{H} :

- (a) the 8 quaternions $\pm e, \pm i, \pm j, \pm k$.
- (b) the 16 quaternions $(\pm e \pm i \pm j \pm k)/2$.
- (c) the 24 quaternions obtained from $(\pm e \pm i)/\sqrt{2}$ by permutations of the symbols e, i, j, k .
- (d) the 24 quaternions obtained by combining the two groups (a), (b) into one.²¹
- (e) the 120 quaternions obtained as the union of the group (d) with 96 quaternions produced from $(\pm e \pm \alpha i \pm \alpha^{-1} j)/2$, where $\alpha = (1 + \sqrt{5})/2$, by all even permutations of the symbols e, i, j, k .

Problem 20.11 (Binary Group of the Icosahedron) Show that the group from [Problem 20.10](#) is isomorphic to $\mathrm{SL}_2(\mathbb{F}_5)$ and admits a surjective homomorphism onto A_5 .

Problem 20.12 (Octaplex) Let $C^4 \subset \mathbb{R}^4$ be the standard regular cocube, i.e., the convex hull of the standard basis vectors and their opposites. Let $Q^4 \subset \mathbb{R}^4$ be a regular cube with the same center as C^4 , with the usual orientation of faces perpendicular to the coordinate axes, but inscribed in the same unit sphere as C^4 . The convex hull of the united vertices of C^4 and Q^4 is called an *octaplex* and

²¹Compare with [Problem 20.12](#) below.

denoted by O^4 . Prove that O^4 is a *regular polyhedron*, meaning that its complete group O_{O^4} acts transitively on the set of *complete flags* formed by a vertex, an edge joined with this vertex, a 2-dimensional face joined with this edge, etc. Calculate: **(a)** the total number of faces in each dimension, **(b)** the lengths of the edges and the radius of the inscribed sphere, **(c)** the area of the 2-dimensional face (and tell which polygon it is), **(d)** the volume of the 3-dimensional face (and tell which polyhedron it is), **(e)** the total volume of O^4 , **(f)** the order of the complete octaplex group $|O_{C^4}|$.

Hints to Selected Exercises

Exercise 1.1 Answer: 2^n .

Exercise 1.2 The answer to the second question is negative. Indeed, let $X = \{1, 2\}$, $Y = \{2\}$. Using unions and intersections, we can obtain only the sets

$$\begin{aligned} X \cap Y &= Y \cap Y = Y \cup Y = Y, \\ X \cup Y &= X \cup X = X \cap X = X. \end{aligned}$$

Thus, each formula built from X , Y , \cap , and \cup produces either $X = \{1, 2\}$ or $Y = \{2\}$. But $X \setminus Y = \{1\}$.

Exercise 1.3 There are six surjections $\{0, 1, 2\} \twoheadrightarrow \{0, 1\}$ and no injections. Symmetrically, there are six injections $\{0, 1\} \hookrightarrow \{0, 1, 2\}$ and no surjections.

Exercise 1.5 If X is finite, then a map $X \rightarrow X$ that is either injective or surjective is automatically bijective. Every infinite set X contains a subset isomorphic to the set of positive integers \mathbb{N} , which admits the nonsurjective injection $n \mapsto (n + 1)$ and the noninjective surjection $1 \mapsto 1, n \mapsto (n - 1)$ for $n \geq 2$. Both can be extended to maps $X \rightarrow X$ by the identity action on $X \setminus \mathbb{N}$.

Exercise 1.6 Use Cantor's diagonal argument: assume that all bijections $\mathbb{N} \cong \mathbb{N}$ are numbered by positive integers, run through this list and construct a bijection that sends each $k = 1, 2, 3, \dots$ to a number different from the image of k under the k -th bijection in the list.

Exercise 1.7 Answer: $\binom{n+m-1}{m-1} = \binom{n+m-1}{n} = \frac{(n+m-1)!}{n!(m-1)!}$. Hint: the summands are in bijection with the numbered collections of nonnegative integers (k_1, k_2, \dots, k_m) such that $\sum k_i = n$. Such a collection is encoded by the word consisting of $(m - 1)$ letters 0 and n letters 1: write k_1 ones, then zero, then k_2 ones, then zero, etc.

Exercise 1.8 Answer: $\binom{n+k}{k}$. A diagram is a broken line going from the bottom left-hand corner of the rectangle to its upper right-hand corner and consisting of n horizontal and k vertical edges.

Exercise 1.9 If z is equivalent to both x and y , then each equivalence $u \sim x$ implies by transitivity and symmetry the equivalence $u \sim y$ and conversely.

Exercise 1.10 Let $[x']_n = [x]_n$ and $[y']_n = [y]_n$, that is, $x' = x + nk$, $y' = y + n\ell$ for some $k, \ell \in \mathbb{Z}$. Then $x' + y' = x + y + n(k + \ell)$ and $x'y' = xy + n(\ell x + ky + k\ell n)$ are congruent modulo n to $x + y$ and xy respectively, i.e., $[x' + y']_n = [x + y]_n$ and $[x'y']_n = [xy]_n$.

Exercise 1.11 Say that $x \sim y$ if there exists a chain satisfying the conditions from [Exercise 1.11](#). Verify that this is an equivalence relation and check that it is a subset of every equivalence relation containing R .

Exercise 1.12 Check of transitivity: if $(p, q) \sim (r, s)$ and $(r, s) \sim (u, w)$, i.e., $ps - rq = 0 = us - rw$, then $psw - rqw = 0 = usq - rwq$, which forces $s(pw - uq) = 0$ and $pw = uq$, i.e., $(p, q) \sim (u, w)$.

Exercise 1.13 Let α be the smaller of the two angles between ℓ_1 and ℓ_2 . Then reflection in ℓ_i followed by reflection in ℓ_j is a rotation about $O = \ell_i \cap \ell_j$ through the angle 2α in the direction from ℓ_i to ℓ_j . Thus, $\sigma_1\sigma_2 = \sigma_2\sigma_1$ if and only if the lines are perpendicular.

Exercise 1.14 The table of products gf is as follows:

| $g \setminus f$ | (1, 2, 3) | (1, 3, 2) | (3, 2, 1) | (2, 1, 3) | (2, 3, 1) | (3, 1, 2) |
|-----------------|-----------|-----------|-----------|-----------|-----------|-----------|
| (1, 2, 3) | (1, 2, 3) | (1, 3, 2) | (3, 2, 1) | (2, 1, 3) | (2, 3, 1) | (3, 1, 2) |
| (1, 3, 2) | (1, 3, 2) | (1, 2, 3) | (3, 1, 2) | (2, 3, 1) | (2, 1, 3) | (3, 2, 1) |
| (3, 2, 1) | (3, 2, 1) | (2, 3, 1) | (1, 2, 3) | (3, 1, 2) | (1, 3, 2) | (2, 1, 3) |
| (2, 1, 3) | (2, 1, 3) | (3, 1, 2) | (2, 3, 1) | (1, 2, 3) | (3, 2, 1) | (1, 3, 2) |
| (2, 3, 1) | (2, 3, 1) | (3, 2, 1) | (2, 1, 3) | (1, 3, 2) | (3, 1, 2) | (1, 2, 3) |
| (3, 1, 2) | (3, 1, 2) | (2, 1, 3) | (1, 3, 2) | (3, 2, 1) | (1, 2, 3) | (2, 3, 1) |

Exercise 1.16 Let $x \in W$ be the minimal element in the set of $w \in W$ for which $\Sigma(w)$ fails. Since $\Sigma(w)$ holds for all $w < x$, then $\Sigma(x)$ must hold as well. Contradiction.

Exercise 1.19 The axiom of choice allows us to choose an upper bound $b(W) \in P$ for every $W \in \mathcal{W}(P)$. If $f(x) > x$ for all $x \in P$, then the map

$$\mathcal{W}(P) \rightarrow P, W \mapsto f(b(W)),$$

contradicts [Lemma 1.2](#) on p. 15.

Exercise 2.2 Answers: $1 + x$ and $xy + x + y$.

Exercise 2.3 It is enough to verify the invariance of the equivalence classes of the results only under changes of fractions by means of the generating relations [\(2.12\)](#), i.e., by $\frac{a}{b} \mapsto \frac{ac}{bc}$.

Exercise 2.5 Use increasing induction on k starting from $k = 0$ to verify that all E_k belong to (a, b) (thus, all E_k are divisible by $\text{GCD}(a, b)$). Then use decreasing

induction on k starting from $k = r + 1$ to verify that all E_k are divisible by E_r (thus, $E_0 = a$, $E_1 = b$, and $\text{GCD}(a, b) = ax + by$ are divisible by E_r).

Exercise 2.8 The existence of a factorization can be proved by induction on $|n|$: If n is prime, its prime factorization is $n = n$; if not, then $n = n_1 \cdot n_2$, where $|n_1|, |n_2| < n$. Thus, n_1, n_2 are factorizable by induction. The proof of the uniqueness is based on the following: for all $z \in \mathbb{Z}$ and prime $p \in \mathbb{Z}$, either $\text{GCD}(z, p) = |p|$ and $p \mid z$ or $\text{GCD}(z, p) = 1$ and p, z are coprime. Given two coinciding products $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$, it follows from Lemma 2.3 on p. 26 that p_1 cannot be coprime to each q_j , because p_1 divides $\prod q_i$. Thus, p_1 divides some q_i , say q_1 . Since q_1 is prime, $q_1 = \pm p_1$. Cancel q_1 and p_1 and repeat the argument.

Exercise 2.9 $a^{-1} = \sum_{k \geq 0} (-1)^k a^k = 1 - a + a^2 - a^3 + \cdots$ (the sum is finite, because a is nilpotent).

Exercise 2.10 The residue class $\binom{p^n m}{p^n} \pmod{p}$ is equal to the coefficient of x^{p^n} in the expansion of the binomial $(1+x)^{p^n m}$ over the finite field $\mathbb{F}_p = \mathbb{Z}/(p)$. Since the map $a \mapsto a^p$ respects sums over \mathbb{F}_p , its n -fold iteration yields $(1+x)^{p^n} = 1 + x^{p^n}$. Hence $(1+x)^{p^n m} = (1+x^{p^n})^m = 1 + mx^{p^n} + \text{higher powers}$.

Exercise 2.12 The axioms are checked componentwise, and they clearly hold because each K_x is a ring.

Exercise 2.13 An element $(a, b) \in \mathbb{F}_p \times \mathbb{F}_q$ is invertible if and only if $a \neq 0$ and $b \neq 0$. A nonzero element $(a, b) \in \mathbb{F}_p \times \mathbb{F}_q$ divides zero if and only if $a = 0$ or $b = 0$.

Exercise 2.17 Both statements follow from Lemma 2.5 on p. 33, which says that every ring homomorphism to an integral domain sends the unit element to the unit element.

Exercise 2.18 Since the polynomial $x^p - x$ is nonzero and of degree p , it has at most p roots¹ in a field \mathbb{F} . Hence, the fixed points of the Frobenius endomorphism $F_p : \mathbb{F} \rightarrow \mathbb{F}$ are exhausted by p elements of the prime subfield $\mathbb{F}_p \subset \mathbb{F}$.

Exercise 3.3 $(y^n - x^n)/(y - x) = y^{n-1} + y^{n-2}x + y^{n-3}x^2 + \cdots + yx^{n-2} + x^{n-1}$.

Exercise 3.5 Let $f(x) = \sum a_k x^k$. Then $f(x+t) = \sum_{k,v} a_k \binom{k}{v} \cdot x^{k-v} t^v = \sum_v t^v \cdot f_v(x)$,

where

$$f_v(x) = \sum_{k \geq v} a_k \binom{k}{v} \cdot x^{k-v} = \frac{1}{v!} \frac{d^k}{dx^k} \sum_{k \geq 0} a_k x^k.$$

Exercise 3.6 The right-hand side is nothing but the output of long division of f by $x - \alpha$. However, now that it has been written down, the equality can easily be checked by straightforward expansion.

Exercise 3.7 Completely similar to Exercise 2.8.

¹See Sect. 3.2 on p. 50.

Exercise 3.8 Completely similar to [Exercise 2.5](#) on p. 25.

Exercise 3.9 A reducible polynomial of degree ≤ 3 has a divisor of degree 1.

Exercise 3.10 Uniqueness follows from [Corollary 3.3](#) on p. 50. To construct f , note that

$$f_i(x) = \prod_{v \neq i} (x - a_v)$$

vanishes at all points a_v except for a_i , at which $f_i(a_i) \neq 0$. Thus $g_i(x) = f_i(x)/f_i(a_i)$ satisfies

$$g_i(a_v) = \begin{cases} 1 & \text{for } v = i, \\ 0 & \text{otherwise.} \end{cases}$$

Hence $f(x) = b_1 g_1 + b_2 g_2 + \cdots + b_n g_n = \sum_{i=0}^n b_i \prod_{v \neq i} \frac{x - a_v}{a_i - a_v}$ solves the problem.

Exercise 3.12 Completely similar to [Exercise 1.10](#) on p. 9.

Exercise 3.13 The canonical embedding $\varphi : \mathbb{k} \hookrightarrow \mathbb{k}[x]/(x - \alpha)$ sends $\alpha \in \mathbb{k}$ to $[\alpha] = [x]$. This forces the equalities $[g(x)] = g([x]) = g([\alpha]) = [g(\alpha)]$ for all $g \in \mathbb{k}[x]$. Thus, $\mathbb{k}[x]/(x - \alpha)$ is exhausted by the classes of constants. That is, the monomorphism φ is surjective.

Exercise 3.14 The inverse of a nonzero expression $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ is

$$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \sqrt{2}.$$

The ring in (a) is not a field, because it has zero divisors:

$$[x + 1] \cdot [x^2 - x + 1] = [0].$$

The ring in (b) is a field by [Proposition 3.8](#).

Exercise 3.15 Use the Euclidean algorithm, which produces $h(x), g(x) \in \mathbb{k}[x]$ such that $h(x)(x - a) + g(x)(x^2 + x + 1) = 1$. Since the remainder on division of $x^2 + x + 1$ by $x - a$ is $a^2 + a + 1$, the algorithm stops at the second step.

Exercise 3.17 Let $\vartheta'_1 = \vartheta_1 + 2\pi k_1$, $\vartheta'_2 = \vartheta_2 + 2\pi k_2$. Then $\vartheta_1 + \vartheta_2 = \vartheta'_1 + \vartheta'_2 + 2\pi(k_1 + k_2)$, as required.

Exercise 3.18 The complex number $\zeta = \cos(2\pi/5) + i \cdot \sin(2\pi/5)$ is a root of the polynomial

$$z^5 - 1 = (z - 1)(z^4 + z^3 + z^2 + z + 1).$$

The reciprocal equation $z^4 + z^3 + z^2 + z + 1 = 0$ can be solved in radicals via division of both of sides by z^2 and a change of variable $z \mapsto t = z + z^{-1}$.

Exercise 3.19 Write $\zeta = \zeta_1 = \cos(2\pi/n) + i\sin(2\pi/n)$ for the root with the smallest positive argument and put $\xi = \zeta^k$, $\eta = \zeta^{\text{GCD}(k,n)}$. Prove the following stronger fact: The sets of all integer powers of ξ and η coincide. Hint: $\zeta^m = \xi^x$ means that $m = kx + ny$ for some $x, y \in \mathbb{Z}$.

Exercise 3.20 The equality $z_1 z_2 = 1$ in $\mathbb{Z}[i]$ forces $|z_1| \cdot |z_2| = 1$ because of $|z|^2 \in \mathbb{N}$ for all $z \in \mathbb{Z}[i]$.

Exercise 3.21 Collect in n_1 all the prime divisors of m_1 whose multiplicity in m_1 is greater than the multiplicity in m_2 .

Exercise 3.23 Write the elements of \mathbb{F}_p in a row as

$$-[(p-1)/2], \dots, -[1], [0], [1], \dots, [(p-1)/2]$$

and check that $a \in \mathbb{F}_p^*$ is a square if and only if the number of “positive” elements that become “negative” after multiplication by a is even (this fact is known as *Gauss’s lemma on quadratic residues*). Then apply this to $a = 2$.

Exercise 4.1 The equality of the fractions $p/q = r/s$ means the equality $ps = qr$ in $\mathbb{k}[x]$. If both representations are simplified, then p and q are coprime, s and r are coprime, and q, s are both monic. It follows from 2.3 that $p = rf$ and $q = sg$ for some $f, g \in \mathbb{k}[x]$. The equality $frs = grs$ forces $f = g$. Since $\text{GCD}(p, q) = \text{GCD}(rg, sg) = 1$, the polynomial g is an invertible constant, forced to be 1 because q and s are both monic.

Exercise 4.3 Compare with formula (3.4) on p. 43.

Exercise 4.4 The rule for differentiating a composition of functions from formula (3.11) on p. 46 implies that $(f^m)' = m \cdot f^{m-1} \cdot f'$ for every f . Thus,

$$\frac{d}{dx}(1-x)^{-m} = \left(\left(\frac{1}{1-x} \right)^m \right)' = m(1-x)^{-m-1}.$$

Now the required formula can be checked by induction.

Exercise 4.7 Differentiate both sides.

Exercise 4.12 Answers: $a_1 = \frac{1}{2}$, $a_2 = \frac{1}{6}$, $a_3 = 0$, $a_4 = -\frac{1}{30}$, $a_5 = 0$, $a_6 = \frac{1}{42}$, $a_7 = 0$, $a_8 = -\frac{1}{30}$, $a_9 = 0$, $a_{10} = \frac{5}{66}$, $a_{11} = 0$, $a_{12} = -\frac{691}{2730}$,

$$S_4(n) = n(n+1)(2n+1)(3n^2+3n-1)/30,$$

$$S_5(n) = n^2(n+1)^2(2n+1)(2n^2+2n-1)/12,$$

$$S_{10}(1000) = 91\,409\,924\,241\,424\,243\,424\,241\,924\,242\,500.$$

Exercise 4.14 Given a finite set f_1, f_2, \dots, f_m of fractional power series $f_i \in \mathbb{k}((x^{1/q_i}))$, they all can be considered simultaneously as elements of the Laurent series field $\mathbb{k}((x^{1/\text{LCM}(f_1, f_2, \dots, f_m)}))$, where all the properties of sums and products involving the set f_1, f_2, \dots, f_m are clearly satisfied.

Exercise 4.15 Let m and $\vartheta(t)$ solve the modified problem. In the case of the first modification, they solve the original problem as well. In the case of the second and third modifications, the original problem is solved by the same m and by the series $\vartheta(t)/a_n(t^q)$ and $\vartheta(t) + a_{n-1}(t^q)/n$ respectively.

Exercise 4.17 Compare with the proof of Proposition 4.5 on p. 99 and remarks before it.

Exercise 5.3 Let polynomials $f(x), g(x) \in I$ have degrees $m \geq n$ and leading coefficients a, b . Then $a + b$ equals either zero or the leading coefficient of the polynomial $f(x) + x^{m-n} \cdot g(x) \in I$ of degree m . Similarly, for every $\alpha \in K$, the product αa is either zero or the leading coefficient of the polynomial $\alpha f(x) \in I$ of degree m .

Exercise 5.4 Repeat the arguments from the proof of Theorem 5.1 but use the lowest nonzero terms instead of the leading ones.

Exercise 5.6 $\sin(2\pi x) / \prod_{\alpha=-k}^k (x - \alpha) \in I_k \setminus I_{k-1}$.

Exercise 5.7 Write I_k for the set of analytic functions vanishing at each point of $\mathbb{Z} \subset \mathbb{C}$ except for integer points m in the range $-k \leq m \leq k$. Then $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$ is an infinite chain of strictly increasing ideals, because of

$$\sin(2\pi z) / \prod_{\alpha=-k}^k (z - \alpha) \in I_k \setminus I_{k-1}.$$

Exercise 5.8 Since I is an additive subgroup of K , the congruence relation $a_1 \equiv a_2 \pmod{I}$ is obviously symmetric, reflexive, and transitive. The correctness of the definitions (5.3) is verified as in Exercise 1.10 on p. 9: if $a' = a + x, b' = b + y$ for some $x, y \in I$, then $a' + b' = a + b + (x + y)$ and $a'b' = ab + (ay + bx + xy)$ are congruent modulo I to $a + b$ and ab respectively.

Exercise 5.9 Write $\pi : K \rightarrow K/I$ for the quotient homomorphism. For an ideal $J \subset K/I$, its preimage $\pi^{-1}(J)$ is an ideal in K . It is generated by some $a_1, a_2, \dots, a_m \in K$. Verify that their residues $[a_v]_I$ span J in K/I .

Exercise 5.11 Each ideal in $\mathbb{C}[x]$ is principal.² If the quotient ring $\mathbb{C}[x]/(f)$ is a field, then f is irreducible. The monic irreducible polynomials in $\mathbb{C}[x]$ are exhausted by the linear binomials $x - \alpha$, where $\alpha \in \mathbb{C}$. The principal ideal $(x - \alpha)$ is equal to $\ker \text{ev}_\alpha$, because $f(\alpha) = 0$ if and only if $x - \alpha$ divides $f(x)$. In $\mathbb{R}[x]$, the principal ideal $\mathfrak{m} = (x^2 + 1)$ is not equal to $\ker \text{ev}_\alpha$ for every $\alpha \in \mathbb{R}$, but $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$ is a field.

Exercise 5.12 Use compactness³ of the segment $[0, 1]$ to show that for every proper ideal $I \subset C$, there exists a point $p \in [0, 1]$ where all functions from I vanish

²Namely, it is generated by the monic polynomial of minimal degree contained in the ideal.

³Every open cover contains a finite subcover.

simultaneously.⁴ This gives an inclusion $I \subset \ker \text{ev}_p$, which has to be an equality as soon as I is maximal. The same holds if $[0, 1]$ is replaced by any compact set X .

Exercise 5.14 If for each k there is $x_k \in I_k \setminus \mathfrak{p}$, then $x_1 \cdot x_2 \cdots x_m \in \bigcap I_k \subset \mathfrak{p}$, whereas $x_k \notin \mathfrak{p}$ for all k . Thus, \mathfrak{p} is not prime.

Exercise 5.15 In (c) and (d), the degree function is multiplicative: $v(z_1 z_2) = v(z_1)v(z_2)$ and $v(z) \geq 1$ for all $z \neq 0$. Hence, $v(z_1 z_2) = v(z_1)$. For every $z \in \mathbb{C}$, there exists w from the ring in question such that $|z - w| < 1$. If we take such w for $z = a/b$, we get $|a - bw| < |b|$. Therefore, property (5.6) holds for $q = w$ and $r = a - bw$.

Exercise 5.16 If $\exists b^{-1}$, then $v(ab) \leq v(abb^{-1}) = v(a)$. Conversely, if $v(ab) = v(a)$, then on division of a by ab , we get $a = abq + r$, where either $v(r) < v(ab) = v(a)$ or $r = 0$. On the other hand, $r = a(1 - bq)$ implies $v(r) \geq v(a)$ as soon as $1 - bq \neq 0$. We conclude that either $1 - bq = 0$ or $r = 0$. In the latter case, $a(1 - bq) = 0$, which forces $1 - bq = 0$ too. Thus, $bq = 1$.

Exercise 5.17 If $b = ax$ and $a = by = axy$, then $a(1 - xy) = 0$, which forces $xy = 1$ as soon as $a \neq 0$.

Exercise 5.18 The polynomials $x, y \in \mathbb{Q}[x, y]$ have no common divisors except for constants. Similarly, the polynomials $2, x \in \mathbb{Z}[x]$ have no common divisors except for ± 1 .

Exercise 5.21 Look at the equality $a_0 q^n + a_1 q^{n-1} p + \cdots + a_{n-1} q p^{n-1} + a_n p^n = 0$.

Exercise 5.22 Answer: $(x^2 - 2x + 2)(x^2 + 2x + 2)$.

Exercise 6.1 If $0 \cdot v = w$, then $w + v = 0 \cdot v + 1 \cdot v = (0 + 1) \cdot v = 1 \cdot v = v$. Add $-v$ to both sides and get $w = 0$. The equality $0 \cdot v = 0$ implies that $\lambda \cdot 0 = \lambda(0 \cdot v) = (\lambda \cdot 0) \cdot v = 0 \cdot v = 0$. The computation $(-1) \cdot v + v = (-1) \cdot v + 1 \cdot v = ((-1) + 1) \cdot v = 0 \cdot v = 0$ shows that $(-1) \cdot v = -v$.

Exercise 6.3 Use increasing induction on m to show that each monomial x^m is a linear combination of f_0, f_1, \dots, f_m . This implies that f_0, f_1, \dots, f_n span $K[x]_{\leq n}$. Then let $\sum \lambda_i f_i = \sum \mu_i f_i$ and compare the coefficients of x^n on both sides. Conclude that $\lambda_n f_n = \mu_n f_n$ can be canceled. Carry out this cancellation and compare the coefficients at x^{n-1} , etc.

Exercise 6.4 If a vector space V over \mathbb{Q} has a countable basis, then as a set, V has the cardinality of the set $\bigcup_{m \geq 0} \mathbb{Q}^m$ of finite sequences of rational numbers, which is countable. But the set $K[[x]]$ has the cardinality of the set $\mathbb{Q}^{\mathbb{N}}$ of infinite sequences of rational numbers, which is uncountable by Cantor's theorem.

Exercise 6.5 Let V be generated by n vectors. By Lemma 6.2 on p. 132, there are at most n linearly independent vectors in V . Conversely, let $e_1, e_2, \dots, e_n \in V$ be a linearly independent set of maximal cardinality. Then for every $v \in V$, there exists a linear relation $\lambda v + \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n = 0$, where $\lambda \neq 0$. Hence, $v = \sum \lambda^{-1} \lambda_i e_i$, and therefore the vectors v_i generate V .

⁴In the contrary case, there exists a finite collection of functions $f_1, f_2, \dots, f_m \in I$ vanishing nowhere simultaneously. Then $\sum f_i^2 \in I$ vanishes nowhere, i.e., it is invertible. This forces $I = C$.

Exercise 6.6 If $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, then $p^m = (p^n)^d = p^{nd}$, where $d = \dim_{\mathbb{F}_{p^n}} \mathbb{F}_{p^m}$.

Exercise 6.7 Let $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m = 0$ for some $v_i \in I = \bigcup_v I_v$, $\lambda_i \in \mathbb{k}$. Since each v_i belongs to some I_{v_i} , all the v_i belong to I_μ for $\mu = \max(v_1, v_2, \dots, v_m)$. Since I_μ is linearly independent, all the λ_i are equal to zero.

Exercise 6.8 Write \mathcal{P} for the set of all pairs (D, J) such that D and J have the same cardinality, $D \subset S$, $J \subset I$, and $I \cup (S \setminus D)$ spans V . The first step in the proof of Lemma 6.2 on p. 132 shows that $\mathcal{P} \neq \emptyset$. The set \mathcal{P} is partially ordered by the relation $(D, J) \leq (D', J')$, meaning that $D \subset D'$ and $J \subset J'$. Show that \mathcal{P} is complete.⁵ By Zorn's lemma, there exists a maximal pair $(D_{\max}, J_{\max}) \in \mathcal{P}$. If $J_{\max} \neq I$, then the same arguments as in the proof of Lemma 6.2 show that $D_{\max} \neq S$, and they allow us to add one more vector to D_{\max} and J_{\max} , in contradiction to the maximality of (D_{\max}, J_{\max}) .

Exercise 6.11 This is a special case of Proposition 7.3 on p. 162. Fix some basis in W and extend it to a basis in V by some vector e , and put ξ as the element of the dual basis corresponding to e . For any two linear forms φ, ψ vanishing on W the linear combination $\varphi(e)\psi - \psi(e)\varphi$ vanishes identically on V .

Exercise 6.12 This follows from Theorem 7.2 on p. 162.

Exercise 6.13 If $W \cup U$ is a subspace of V and there is a vector $w \in W \setminus U$, then for all $u \in U$, $w + u \in W \cup U$ but $w + u \notin U$. This forces $w + u \in W$ and $u \in W$. Thus, $U \subset W$.

Exercise 6.14 Every vector $w \in V$ can be written as $w = \frac{\xi(w)}{\xi(v)} \cdot v + u$, where $u = w - \frac{\xi(w)}{\xi(v)} \cdot v \in \ker \xi$, because $\xi\left(w - \frac{\xi(w)}{\xi(v)} \cdot v\right) = \xi(w) - \frac{\xi(w)}{\xi(v)} \cdot \xi(v) = 0$.

Exercise 6.15 Use induction on the number of subspaces. The key case of two subspaces is covered by Corollary 6.8 on p. 140.

Exercise 6.16 Since each vector $v \in V$ has a unique representation as a sum $v = \sum u_i$ with $u_i \in U_i$, the addition map $\oplus U_i \rightarrow V$, $(u_1, u_2, \dots, u_m) \mapsto \sum u_i$, is bijective. Clearly, it is also linear.

Exercise 6.17 Use the equalities $\vec{p}\vec{r} + \vec{r}\vec{s} = \vec{p}\vec{s} = \vec{p}\vec{q} + \vec{q}\vec{s}$.

Exercise 6.20 The center of mass c for the total collection of all points p_i, q_j is defined by

$$\sum_i \lambda_i \vec{c}\vec{p}_i + \sum_j \mu_j \vec{c}\vec{q}_j = 0.$$

Substitute $\vec{c}\vec{p}_i = \vec{c}\vec{p} + \vec{p}\vec{p}_i$, $\vec{c}\vec{q}_j = \vec{c}\vec{q} + \vec{q}\vec{q}_j$ in this equality and use the conditions $\sum \lambda_i \vec{p}\vec{p}_i = 0$, $\sum \mu_j \vec{q}\vec{q}_j = 0$ to get $\left(\sum \lambda_i\right) \vec{c}\vec{p} + \left(\sum \mu_j\right) \vec{c}\vec{q} = 0$.

Exercise 6.23 Similar to Exercise 5.8 on p. 106.

Exercise 6.24 Bijectivity means that $F(v) = F(w) \iff v - w \in \ker F$.

⁵Compare with Exercise 6.7 on p. 134.

Exercise 6.26 If $a_1 - a_2 \in B$, then $\lambda a_1 - \lambda a_2 = \lambda(a_1 - a_2) \in B$ as soon as $\lambda \cdot B \subset B$.

Exercise 7.5 If some finite linear combination $\sum_i \lambda_i (1 - \alpha_i t)^{-1}$ vanishes in $\mathbb{k}[[t]]$, then $\sum_i \lambda_i \prod_{v \neq i} (1 - \alpha_v t) = 0$ in $\mathbb{k}[t]$. The substitution $t = \alpha_i^{-1}$ leads to the equality $\lambda_i = 0$.

Exercise 7.6 The vectors v_1, v_2, \dots, v_n are linearly independent, because an evaluation of ξ_i on both sides of the linear relation $\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n = 0$ shows that $\lambda_i = 0$, and this holds for each i . Since $\dim V = n$, the vectors v_1, v_2, \dots, v_n form a basis. The relations $\varphi_i(v_i) = 1$ and $\varphi_i(v_j) = 0$ for $i \neq j$ say that $\varphi_1, \varphi_2, \dots, \varphi_n$ form the dual basis in V^* .

Exercise 7.7 Include w as a basic vector in some basis of W and take ξ to be the coordinate form w^* along w .

Exercise 7.8 If a linear form vanishes on some vectors, then it vanishes on all linear combinations of those vectors.

Exercise 7.12 $\langle v, G^* F^* \xi \rangle = \langle Gv, F^* \xi \rangle = \langle FGv, \xi \rangle$.

Exercise 8.1 For units $e', e'' \in A$, we have $e' = e' \cdot e'' = e''$. For all $a, b \in A$ we have $0 \cdot a = (b + (-1) \cdot b)a = ba + (-1)ba = 0$.

Exercise 8.2 We have

$$E_{ij}E_{k\ell} = \begin{cases} E_{i\ell} & \text{for } j = k, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, $E_{12}E_{21} \neq E_{21}E_{12}$. The complete list of commutation relations among the E_{ij} looks like this:

$$[E_{ij}, E_{k\ell}] \stackrel{\text{def}}{=} E_{ij}E_{k\ell} - E_{k\ell}E_{ij} = \begin{cases} E_{ii} - E_{jj} & \text{for } j = k \text{ and } i = \ell, \\ E_{i\ell} & \text{for } j = k \text{ and } i \neq \ell, \\ -E_{kj} & \text{for } j \neq k \text{ and } i = \ell, \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 8.5 Let $AB = C$, $B'A' = D$. Then $c_{ij} = \sum_k a_{ik}b_{kj} = \sum_k a'_{ki}b'_{jk} = \sum_k b'_{jk}a'_{ki} = d_{ji}$.

Exercise 8.8 Write u_1, u_2, \dots, u_r for the nonzero rows of the reduced echelon matrix in question and j_1, j_2, \dots, j_r for its shape. Then the j_k th coordinate of $\sum \lambda_v u_v$ equals λ_k for all $k = 1, 2, \dots, r$. Thus $\sum \lambda_v u_v = 0$ only if all λ_v are equal to zero.

Exercise 8.9 The projection $p : \mathbb{k}^n \twoheadrightarrow E_J$ along E_I maps U onto the linear span of the rows of the submatrix formed by the columns indexed by J . The latter coincides with the whole of E_J if and only if its dimension satisfies $\dim E_J = r$.

Exercise 8.10 The original system is recovered from the transformed one by an elementary transformation of the same type.

Exercise 8.11 Each $d_i = \dim \pi_i(U)$ is equal to the number of nonzero rows in the submatrix of A formed by the first i columns.

Exercise 8.12 A vector subspace of codimension $r^2 + \sum_{v=1}^r (j_v - v + 1)$ in $\text{Mat}_{r \times n}(\mathbb{k})$ is formed by matrices having zeros in the columns (j_1, j_2, \dots, j_r) and at the first j_v positions of the v th row for each $v = 1, \dots, r$. A shift of this subspace by the matrix E_I , which has the unit $r \times r$ submatrix in the columns (j_1, j_2, \dots, j_r) and zeros in all other positions, consists exactly of reduced echelon matrices of combinatorial type (j_1, j_2, \dots, j_r) .

Exercise 8.15 The inverse matrix is
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -5 & 2 \\ 0 & 0 & -17 & 7 \end{pmatrix}.$$

Exercise 8.16 See [Exercise 8.1](#).

Exercise 8.18 Verify that $\det(FG) = \det F \cdot \det G$ for 2×2 matrices. This forces $\det F$ to be invertible for invertible F , because of $\det F \cdot \det F^{-1} \det(FF^{-1}) = \det E = 1$. If $\det F$ is invertible, then formula (8.7) can be proved by the same arguments as in Example 8.5.

Exercise 8.19 Use the equalities

$$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} b & 0 \\ d & c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Exercise 9.1 Write a permutation $g = (g_1, g_2, \dots, g_n)$ of symbols $\{1, 2, \dots, n\}$ as $g = \sigma \circ g'$, where σ swaps the symbols n and g_n . Then $g' = \sigma \circ g$ preserves the symbol n . By induction, g' equals a composition of transpositions preserving n .

Exercise 9.2 If only transversal double crossings of threads are allowed, two threads drawn from i and j have an odd number of intersections⁶ if and only if the pair (i, j) is reversed by g . For a shuffle permutation $(i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_m)$, the threads going from i_1, i_2, \dots, i_k do not intersect each other but do intersect, respectively, $i_1 - 1, i_2 - 2, \dots, i_k - k$ threads going from j -points situated on the left. Since those j -threads also do not intersect each other,

$$\text{sgn}(i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_m) = \sum_v (i_v - v).$$

⁶In fact, the threads can always be drawn in such a way that this number equals either 0 or 1 for any two threads.

Exercise 9.3 If $g = \sigma_1 \cdot \sigma_2 \cdots \sigma_k$, where all s_i are transpositions, then $h = s_k \cdots s_2 s_1$ satisfies the equalities $hg = gh = \text{Id}$, because of $s_i s_i = \text{Id}$ for all i . Hence, $g^{-1} = h$ and $\text{sgn}(g^{-1}) = (-1)^k = \text{sgn}(g)$.

Exercise 9.5 Write v_1, v_2, \dots, v_n for the columns of C . The condition $\text{rk } C < n$ implies that these vectors are linearly related. For instance, let $v_1 = \sum_{k \geq 2} \lambda_k v_k$. Then $\det(v_1, v_2, \dots, v_n) = \sum_{k \geq 2} \lambda_k \det(v_k, v_2, \dots, v_n) = 0$.

Exercise 9.6 Use induction on m . For $m = 1$, the vanishing condition means that $f \in \mathbb{k}[x]$ has more than $\deg f$ roots. Hence $f = 0$ by Corollary 3.2 on p. 50. For $m > 1$, write $f \in \mathbb{k}[x_1, x_2, \dots, x_m]$ as a polynomial in x_m with coefficients in $\mathbb{k}[x_1, x_2, \dots, x_{m-1}]$ and evaluate the coefficients at an arbitrary point $q \in \mathbb{k}^{m-1}$. This leads to a polynomial in $\mathbb{k}[x_m]$ vanishing at each point of \mathbb{k} . Hence, it must be the zero polynomial. This forces each coefficient of f to vanish at all $q \in \mathbb{k}^{m-1}$. By induction, all coefficients have to be zero polynomials, i.e., $f = 0$.

Exercise 9.8 If $\det F \neq 0$, then $\dim \text{im } F = \dim V$, because otherwise, $\det F = 0$ by Exercise 9.5. Thus F is surjective and hence invertible if $\det F \neq 0$. In this case, $\det F \cdot \det F^{-1} = \det \text{Id} = 1$.

Exercise 9.9 To move each ξ_j through all the ξ_i from right to left, one needs m transpositions.

Exercise 9.10 For even n , such a basis consists of all monomials of even degree, while for odd n , it consists of even-degree monomials and the highest-degree monomial $\xi_1 \wedge \xi_2 \wedge \cdots \wedge \xi_n$, which has odd degree.

Exercise 9.11 Just transpose everything and use the equality $\det A = \det A'$.

Exercise 9.12 The result follows at once from Proposition 9.3 and Corollary 6.4 on p. 136.

Exercise 10.1 Linearity is a basic property of the integral. Positivity holds because a nonzero nonnegative continuous function is positive over some interval.

Exercise 10.2 The linear form g_{e_j} sends the basis vector e_i to (e_i, e_j) . Thus, the i th coordinate of this form in the dual basis equals (e_i, e_j) .

Exercise 10.5 If u and w either are linearly independent or have $(u, v) < 0$, then strict inequality holds in the computation made two rows below formula (10.21) on p. 239.

Exercise 10.6 The Euclidean dual basis to the basis $u_1 = 1, u_2 = t, u_3 = t^2$ in U is formed by vectors u_j^\vee whose coordinates in the basis u_i are in the columns of the matrix

$$C_{uu^\vee} = G_u^{-1} = \begin{pmatrix} 1 & 1/2 & 1/3 \\ 1/2 & 1/3 & 1/4 \\ 1/3 & 1/4 & 1/5 \end{pmatrix}^{-1} = \begin{pmatrix} 9 & -36 & 30 \\ -36 & 192 & -180 \\ 30 & -180 & 180 \end{pmatrix}.$$

By Theorem 10.1, the orthogonal projection $\pi_U v = \sum (v, u_i) \cdot u_i^\vee$ has coordinates

$$-\frac{1}{4} \cdot \begin{pmatrix} 9 \\ -36 \\ 30 \end{pmatrix} - \frac{1}{5} \cdot \begin{pmatrix} -36 \\ 192 \\ -180 \end{pmatrix} - \frac{1}{6} \cdot \begin{pmatrix} 30 \\ -180 \\ 180 \end{pmatrix} = \begin{pmatrix} -1/20 \\ 3/5 \\ -3/2 \end{pmatrix}$$

in the basis u_1, u_2, u_3 . Thus, the required polynomial is

$$f(t) = t^3 + \pi_U v = t^3 - \frac{3}{2}t^2 + \frac{3}{5}t - \frac{1}{20},$$

and the value of the integral $\int_0^1 f^2(t) dt$ is equal to

$$\begin{pmatrix} -1/20 & 3/5 & -3/2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{pmatrix} \cdot \begin{pmatrix} -1/20 \\ 3/5 \\ -3/2 \\ 1 \end{pmatrix} = \frac{1}{2800}.$$

Exercise 10.9 The transition matrix has $\det \begin{pmatrix} 1/|u| & * \\ 0 & 1/|v| \end{pmatrix} > 0$.

Exercise 10.10 Let $\Pi_1 = a + W_1$, $\Pi_2 = b + W_2$. Since $W_1 \neq W_2$, $\dim(W_1 \cap W_2) < \dim W_1 = \dim V - 1$. Hence

$$\begin{aligned} \dim(W_1 + W_2) &= \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2) \\ &> 2(\dim V - 1) - (\dim V - 1) = \dim V - 1. \end{aligned}$$

This forces $\dim(W_1 + W_2) = \dim V$, that is, $V = W_1 + W_2$ and $\dim(W_1 \cap W_2) = \dim V - 2$. The intersection

$$\Pi_1 \cap \Pi_2 = \{a + W_1\} \cap \{b + W_2\}$$

is not empty, because there are some $w_i \in W_i$ such that $a - b = w_2 - w_1$, that is, $a + w_1 = b + w_2$.

Exercise 10.12 The first three statements are obvious from formula (10.27) on p. 246, while the fourth follows immediately from the second and the third: writing $v \in V$ as $v = \lambda e + u$, where $u \in e^\perp$, we get $|\sigma_e(v)| = |u - \lambda e| = \sqrt{|u|^2 + \lambda^2} = |u + \lambda e| = |v|$.

Exercise 10.13 Vectors $a, b \in V$ with $|a| = |b| \neq 0$ are transposed by the reflection in the middle perpendicular hyperplane⁷ to $[a, b]$. To prove the second statement,

⁷See Example 10.7 on p. 241.

use induction on $n = \dim V$. The base case $n = 1$ is trivial.⁸ In the generic case, choose an arbitrary nonzero vector $v \in V$ and compose a given isometry F with a reflection σ sending Fv to v . Since σF preserves v , it sends the $(n-1)$ -dimensional subspace v^\perp to itself. By induction, the restriction of σF to v^\perp is a composition of at most $(n-1)$ reflections. The latter can be extended to reflections of the whole space V in the hyperplanes containing v . Thus, $\sigma F : V \xrightarrow{\sim} V$ is a composition of at most $(n-1)$ reflections. Hence $F = \sigma\sigma F$ is a composition of at most n reflections.

Exercise 11.2 The cardinality of the left-hand side is equal to the number of nonzero vectors in \mathbb{F}_q^{n+1} divided by the number of nonzero vectors in a line, that is, it is equal to $(q^{n+1} - 1)/(q - 1)$. On the right-hand side is $q^n + q^{n-1} + \cdots + q + 1$. A good reason to call it a *geometric* progression, isn't it?

Exercise 11.3 In terms of polynomials, a change of basis in V^* means a linear change of variables (x_0, x_1, \dots, x_n) by variables $(y_0, y_1, \dots, y_n) = (x_0, x_1, \dots, x_n) \cdot C$, where $C \in \text{Mat}_n(\mathbb{k})$ is some invertible matrix. Since each monomial in y can be written as a combination of monomials in x , the function $V \rightarrow \mathbb{k}$ produced by a monomial in y lies in the linear span of functions produced by monomials in x . Since C is invertible, the converse statement is also true. Thus, the linear spans of the polynomial functions produced by the monomials in x and in y coincide.

Exercise 11.8 Answer: $\binom{n+d}{d} - 1$ if $\dim V = n + 1$.

Exercise 11.9 Let $L_1 = \mathbb{P}(U)$, $L_2 = \mathbb{P}(W)$, $p = \mathbb{P}(\mathbb{k} \cdot e)$. Since $p \notin V = W \oplus \mathbb{k} \cdot e$. The projection in question is induced by the linear projection of V onto W onto W along $\mathbb{k} \cdot e$. Since $\mathbb{k} \cdot e \cap L_1 = 0$, the restriction of this linear subspace U has zero kernel.

Exercise 11.10 Write φ_p (respectively φ_q) for the linear fractional transformations sending p_1, p_2, p_3 (respectively q_1, q_2, q_3) to $\infty, 0, 1$. If $[p_1, p_2, p_3, p_4] = [q_1, q_2, q_3, q_4]$, then $\varphi_p(p_4) = \varphi_q(q_4)$, and the composition $\varphi_q^{-1} \circ \varphi_p$ sends p_1, p_2, p_3, p_4 to q_1, q_2, q_3, q_4 . Conversely, if there is a linear fractional transformation φ_{qp} sending p_i to q_i , then the composition $\varphi_p \circ \varphi_{qp}^{-1}$ takes q_1, q_2, q_3, q_4 to $\infty, 0, 1, [p_1, p_2, p_3, p_4]$ respectively. This forces $[p_1, p_2, p_3, p_4] = [q_1, q_2, q_3, q_4]$.

Exercise 12.2 If, then

Exercise 12.3 Taking $h_1 = h_2 = h$ for some $h \in H$, we conclude that $e \in H$. Taking $h_1 = e, h_2 = h$, we conclude that $h^{-1} \in H$ for all $h \in H$. Taking $h_1 = g, h_2 = h^{-1}$, we conclude that $gh \in H$ for all $g, h \in H$.

Exercise 12.4 $\text{Aut}G = \text{GL}_1(\mathbb{F}_p) = \mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)$.

Exercise 12.5 Answer: $n(n-1)\cdots(n-m+1)/m$ (the numerator consists of m factors).

Exercise 12.6 Let $k = dr, m = ds$, where $d \in \mathbb{N}$ and $\text{GCD}(r, s) = 1$. If $d > 1$, then τ^d splits into d nonintersecting cycles of length s , and $\tau^k = (\tau^d)^r$ is the composition

⁸See Example 10.10 on p. 245.

of the r powers of these cycles. If $\text{GCD}(m, k) = 1$, consider an arbitrary element a appearing in τ and write r for the minimal positive exponent such that $(\tau^k)^r a = a$. Then $m \mid kr$. Hence, $m \mid r$. Therefore, $r \geq m$. This forces τ^k to be a cycle of length m .

Exercise 12.7 Let cycles τ_1, τ_2 commute and have a common element a . Then $\tau_1(a)$ also lies in τ_2 , because otherwise, $\tau_2\tau_1(a) = \tau_1(a)$ but $\tau_2(a) \neq a$ forces $\tau_1\tau_2(a) \neq \tau_1(a)$. For the same reason, $\tau_2(a)$ lies in τ_1 . Hence, both cycles consist of the same elements. In particular, they have equal lengths. Let $\tau_1(a) = \tau_2^s(a)$. Then each element b appearing in the cycles can be written as $b = \tau_2^r(a)$, and τ_1 acts on b exactly as τ_2^s does:

$$\tau_1(b) = \tau_1\tau_2^r(a) = \tau_2^r\tau_1(a) = \tau_2^r\tau_2^s(a) = \tau_2^s\tau_2^r(a) = \tau_2^s(b).$$

Thus, $\tau_1 = \tau_2^s$, and by [Exercise 12.6](#), s is coprime to the length of the cycles.

Exercise 12.8 Two of the $n!$ fillings of a given Young diagram produce equal permutations⁹ if they are obtained from each other by cyclically permuting the elements within rows or arbitrarily permuting rows of equal lengths in their entirety (compare with formula (1.11) on p. 7).

Exercise 12.9 $|1, 6, 3, 4\rangle^{15} \cdot |2, 5, 8\rangle^{15} \cdot |7, 9\rangle^{15} = |1, 6, 3, 4\rangle^{-1} \cdot |7, 9\rangle = (4, 2, 6, 3, 5, 1, 9, 8, 7).$

Exercise 12.13 Answer: $|1, 2, 3, 4\rangle = \sigma_{12}\sigma_{23}\sigma_{34}$, $|1, 2, 4, 3\rangle = \sigma_{12}\sigma_{24}\sigma_{34}$, $|1, 3, 2, 4\rangle = \sigma_{13}\sigma_{23}\sigma_{24}$, $|1, 3, 4, 2\rangle = \sigma_{13}\sigma_{34}\sigma_{24}$, $|1, 4, 2, 3\rangle = \sigma_{24}\sigma_{23}\sigma_{13}$, $|1, 4, 3, 2\rangle = \sigma_{34}\sigma_{23}\sigma_{12}$.

Exercise 12.15 The calculations for the cube are similar to those for the tetrahedron and dodecahedron. The groups of the octahedron are isomorphic to the groups of the cube with vertices in the centers of the octahedral faces. The same holds for the icosahedron and dodecahedron (just look at the models you made in [Exercise 12.10](#)).

Exercise 12.16 Fix a basis in V and send the operator $F \in \text{GL}(V)$ to the basis formed by vectors $f_i = F(e_i)$. The first vector f_1 of that basis can be chosen in $|V| - 1 = q^n - 1$ ways, the second in $|V| - |\mathbb{k} \cdot f_1| = q^n - q$ ways, the third in $|V| - |\mathbb{k} \cdot f_1 \oplus \mathbb{k} \cdot f_2| = q^n - q^2$ ways, etc.

Exercise 12.17 Each vertex of the dodecahedron belongs to exactly two of five cubes. These two cubes have exactly two common vertices, and these vertices are opposite vertices of the dodecahedron. Therefore, a rotation preserving two cubes is forced to be a rotation about the axis passing through the common opposite vertices of the cubes. Taking the other two cubes, we conclude that the only proper isometry preserving four cubes is the identity map.

Exercise 12.18 Hint: The central symmetry commutes with all elements of O_{dod} , whereas in S_5 there are no such elements except for the unit.

⁹Assuming that the permutation obtained from such a filling is the product of cycles written in rows and read from left to right.

Exercise 12.23 We sketch the arguments for the case of the icosahedron. The icosahedral group acts transitively on the 20 faces of the icosahedron. The stabilizer of a face in the complete (respectively proper) icosahedral group is the complete (respectively proper) group of the regular triangle in the Euclidean plane. Therefore, $|\mathrm{O}_{\mathrm{ico}}| = 20 \cdot 6 = 120$ (respectively $|\mathrm{SO}_{\mathrm{ico}}| = 20 \cdot 3 = 60$).

Exercise 12.24 Since elements $g_1 g_2^{-1}$, $g_2 g_1^{-1}$ are inverse to each other, if one of them lies in H , then the other lies there, too. The equality $h_1 g_1 = h_2 g_2$ forces $g_1 g_2^{-1} = h_1^{-1} h_2 \in H$. Conversely, if $g_1 g_2^{-1} = h \in H$, then $H g_1 = H h g_2 = H g_2$, because $H h = H$ for all $h \in H$.

Exercise 12.25 The inclusion $g H g^{-1} \subset H$ is equivalent to the inclusion $H \subset g^{-1} H g$. If this holds for all $g \in G$, then we can substitute g by g^{-1} in the second inclusion and get $g H g^{-1} \supset H$.

Exercise 12.26 $\varphi \circ \mathrm{Ad}_g \circ \varphi^{-1} : h \mapsto \varphi(g \varphi^{-1}(h) g^{-1}) = \varphi(g) h \varphi(g)^{-1}$.

Exercise 12.27 Let $q \in \mathbb{A}(V)$ and $p = \varphi^{-1}(q)$. Then $\varphi(p + v) = q + D_\varphi(v)$ and

$$\varphi \circ \tau_v \circ \varphi^{-1} : q \mapsto \varphi(p + v) = q + D_\varphi(v).$$

Exercise 12.29 If $\varphi(x) \in N_2$, then $\varphi(g x g^{-1}) = \varphi(g) \varphi(x) \varphi(g)^{-1} \in N_2$, because $N_2 \triangleleft G_2$ is normal. Hence, $N_1 = \varphi^{-1}(N_2) \triangleleft G_1$. The composition of surjective homomorphisms $G_1 \twoheadrightarrow G_2 \twoheadrightarrow G_2/N_2$ is a surjection with kernel N_1 .

Exercise 13.2 Write ε for the variable taking the values ± 1 . When we insert $x^\varepsilon x^{-\varepsilon}$ in some word w , we get a word in which removal of any fragment $y^\varepsilon y^{-\varepsilon}$ leads either back¹⁰ to w or to a word obtained from w by removal of the same fragment $y^\varepsilon y^{-\varepsilon}$ followed by inserting $x^\varepsilon x^{-\varepsilon}$ at the same place as in w .

Exercise 13.3 Send $n \in \mathbb{N}$ to $x^n y x^n \in F_2$ and use Proposition 13.1 on p. 310.

Exercise 13.5 Multiply both sides by the word from the right-hand side written in the reverse order. This leads either to $(x_1 x_2)^n = e$ or to $x_2 (x_1 x_2)^n x_2^{-1} = e$.

Exercise 13.6 If some geodesic passes through some vertex v of the triangulation, then it breaks the $2m_i$ edges outgoing from v in two parts, each consisting of m_i edges, such that any two edges cut by the same reflection plane occur in different parts. Therefore, when we vary a or b and the geodesic (a, b) meets the vertex v , a fragment of length m_i in w is replaced by the complementary fragment of the same length m_i . This proves the first statement. The second can be proved by induction on the length of the word representing g . If it is zero, then $g = e$, and there is nothing to prove. Assume that the statement is true for all g representable by a word of length at most n . It is enough to show that it holds for all elements $g\sigma_i$. Triangle $g\sigma_i$ is obtained from triangle g by reflection in the plane $g(\pi_i)$, which passes through their common side and breaks the sphere into two hemispheres. If triangles $g\sigma_i$ and e lie in the same hemisphere, we can choose points a, b, b' in triangles $e, g\sigma_i, g$ in such a

¹⁰Note that this may happen not only when we remove exactly the same fragment $x^\varepsilon x^{-\varepsilon}$ that was just inserted; sometimes, one of the letters $x^{\pm\varepsilon}$ can be canceled by another neighbor.

way that the shortest geodesic a, b' passes through b and crosses the common side of triangles $g\sigma_i, g$. This geodesic produces words w and wx_i such that $\varphi(w) = g\sigma_i$ and $\varphi(wx_i) = g$. By induction, wx_i is the shortest word for g . Since $g\sigma_i$ is represented by an even shorter word, the statement holds for $g\sigma_i$ by induction as well. If triangles $g\sigma_i$ and e lie in different hemispheres, then the shortest geodesic from e to $g\sigma_i$ can be chosen coming into triangle $g\sigma_i$ from triangle g through their common side. This geodesic produces words wx_i and w for $g\sigma_i$ and g . If wx_i is equivalent to some shorter word, then the latter is of length at most n , and the statement holds for $g\sigma_i$ by induction. There remains to consider only the case that wx_i is the shortest word for $g\sigma_i$. But that is exactly what we need.

Exercise 13.7 If the first statement is not evident, see Sect. 13.2.2 on p. 321. Relations $\sigma_i^2 = e$ and $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i - j| \geq 2$ are obvious. It suffices to verify the relation $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ only in $S_3 = D_3$.

Exercise 13.8 Let $\mathbb{A}^n = \mathbb{A}(V)$ and write (p_0, p_1, \dots, p_n) and (q_0, q_1, \dots, q_n) for the points in question. As we have seen in Sect. 6.5.5 on p. 148, the required map $\mathbb{A}(V) \rightarrow \mathbb{A}(V)$ takes $x \mapsto q_0 + F(\overrightarrow{p_0x})$, where $F : V \rightarrow V$ is some linear map sending $\overrightarrow{p_0p_i}$ to $\overrightarrow{q_0q_i}$ for all $1 \leq i \leq n$. Since both collections of vectors $\overrightarrow{p_0p_i}$ and $\overrightarrow{q_0q_i}$ form bases of V , a linear map F exists and is unique and bijective.

Exercise 13.9 Let $v_i = \overrightarrow{ce_i} = e_i - c$ be the radius vector of vertex i in \mathbb{R}^{n+1} . Then $n_{ij} = v_i - v_j$ is orthogonal to the hyperplane π_{ij} , because for every $k \neq i, j$, the inner product is given by

$$(n_{ij}, v_k - (v_i + v_j)/2) = (v_i, v_k) - (v_j, v_k) + (v_i, v_i)/2 - (v_j, v_j)/2 = 0$$

(products (v_i, v_j) for $i \neq j$ and squares (v_i, v_i) do not depend on i, j by symmetry). A similar computation shows that n_{ij} and n_{km} are orthogonal for $\{i, j\} \cap \{k, m\} = \emptyset$. Vectors $v_i - v_k$ and $v_k - v_j$ span the Euclidean plane, where they are the sides of an equilateral triangle with vertices v_i, v_j, v_k . Therefore, the angle between n_{ik} and n_{kj} equals 60° .

Exercise 13.10 The argument is word for word the same as in Exercise 13.6.

Exercise 13.11 If $I(g) = 0$, then g has no inversions. If $I(g) = n(n+1)/2$, then all the pairs must be reversed for g .

Exercise 13.14 An epimorphism $S_4 \rightarrow D_3$ from Example 12.10 on p. 291 maps $A_4 \subset S_4$ onto the cyclic subgroup of rotations.

Exercise 13.15 Since $C \triangleleft D$, the product $(A \cap D)C$ is a normal subgroup of D by Proposition 12.5 on p. 302. The isomorphism $HN/N \simeq H/H \cap N$ from Proposition 12.5 for $G = D$, $H = B \cap D$, $N = (A \cap D)C$ is the required $(B \cap D)C/(A \cap D)C \simeq (B \cap D)/(A \cap D)(B \cap C)$, because for $A \subset B$, we have $HN = (B \cap D)(A \cap D)C = (B \cap D)C$, and the equality $H \cap N = (B \cap D) \cap (A \cap D)C = (A \cap D)(B \cap C)$ holds (any element $d = ac \in (B \cap D) \cap (A \cap D)$, where $d \in B \cap D$, $a \in A \cap D$, $c \in C$, has $c = a^{-1}d \in C \cap B$).

Exercise 13.16 The requisite odd permutation is either a transposition of two fixed elements or a transposition of two elements forming a cycle of length 2.

Exercise 13.17 For every 5-cycle τ there is some $g \in S_5$ such that $g\tau g^{-1} = |1, 2, 3, 4, 5\rangle$. If g is odd, then $h\tau h^{-1} = |2, 1, 3, 4, 5\rangle$ for even $h = \sigma_{12}g$. The assignment $\tau \mapsto \sigma_{12}\tau\sigma_{12}$ establishes a bijection between 5-cycles conjugate to $|1, 2, 3, 4, 5\rangle$ in A_5 and 5-cycles conjugate to $|2, 1, 3, 4, 5\rangle$.

Exercise 13.18 Reducing $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$ modulo 3, 4, and 5, we get $1 - \varepsilon_3$, $1 - \varepsilon_4$, and $1 + 2(\varepsilon_1 + \varepsilon_2)$ respectively. Thus, H is divisible by 3 or 4 only if $\varepsilon_3 = 1$ or $\varepsilon_4 = 1$. In both cases, $|H| \geq 16$. Hence, $|H|$ is neither 3 nor 4 nor $3 \cdot 4$ nor $3 \cdot 5$. If $|H| \vdots 5$, then $\varepsilon_1 = \varepsilon_2 = 1$ and $|H| \geq 25$. Hence, $|H|$ is neither 5 nor $4 \cdot 5$. The remaining possibilities are only $|H| = 1$ and $|H| = 3 \cdot 4 \cdot 5$.

Exercise 13.20 Choose $k \notin i, j, g^{-1}(i)$. Then $g(k) = m \notin \{i, j, k\}$. If $n \geq 6$, there exists an even permutation h that preserves i, j, k and sends m to some $\ell \neq m$. Then hgh^{-1} maps $i \mapsto j$ and $k \mapsto \ell \neq m$.

Exercise 13.21 Associativity is checked as follows:

$$\begin{aligned} ((x_1, h_1) \cdot (x_2, h_2)) \cdot (x_3, h_3) &= (x_1\psi_{h_1}(x_2), h_1h_2) \cdot (x_3, h_3) \\ &= (x_1\psi_{h_1}(x_2)\psi_{h_1h_2}(x_3), h_1h_2h_3), \\ (x_1, h_1) \cdot ((x_2, h_2) \cdot (x_3, h_3)) &= (x_1, h_1) \cdot (x_2\psi_{h_2}(x_3), h_2h_3) \\ &= (x_1\psi_{h_1}(x_2\psi_{h_2}(x_3)), h_1h_2h_3), \end{aligned}$$

and $\psi_{h_1}(x_2\psi_{h_2}(x_3)) = \psi_{h_1}(x_2)\psi_{h_1} \circ \psi_{h_2}(x_3) = \psi_{h_1}(x_2)\psi_{h_1h_2}(x_3)$. Multiplication by the unit yields $(x, h) \cdot (e, e) = (x, \psi_h(e), he) = (x, h)$, because $\psi_h(e) = e$ (ψ_h is a group homomorphism). What about the inverse element, $(\psi_h^{-1}(x^{-1}), h^{-1}) \cdot (x, h) = (\psi_h^{-1}(x^{-1})\psi_h^{-1}(x), h^{-1}h) = (e, e)$?

Exercise 13.22 Since $\psi_e = \text{Id}_N$ (because $\psi : H \rightarrow \text{Aut } N$ is a homomorphism), we have $(x_1, e) \cdot (x_2, e) = (x_1\psi_e(x_2), e) = (x_1x_2, e)$.

Hence, N' is a subgroup and is isomorphic to N . The normality of N' is checked as follows:

$$(y, h) \cdot (x, e) \cdot (\psi_h^{-1}(y^{-1}), h^{-1}) = (y\psi_h(x), h) \cdot (\psi_h^{-1}(y^{-1}), h^{-1}) = (y\psi_h(x)y^{-1}, e).$$

All the statements about H' are evident. The isomorphism $N' \rtimes H' \simeq N \rtimes_{\psi} H$ holds because $\text{Ad}_{(e, h)}(x, e) = (\psi_h(x), e)$.

Exercise 13.23 Write G for the group and $C = Z(G)$ for its center. If $|C| = p$, then $C \simeq \mathbb{Z}/(p) \simeq G/C$. Let C be generated by $a \in C$ and G/C be generated by bC for some $b \in G$. Then every element of G can be written as $b^k a^m$. Since a commutes with b , any two such elements commute.

Exercise 13.24 For every $k \in \mathbb{Z}$, the multiplication-by- $m \in \mathbb{Z}$ map

$$m : \mathbb{Z}/(k) \rightarrow \mathbb{Z}/(k), \quad [x] \mapsto m[x] \stackrel{\text{def}}{=} \underbrace{[x] + \cdots + [x]}_m = [mx],$$

is a well-defined endomorphism of the additive group $\mathbb{Z}/(k)$. For $k = m$, it takes the whole of $\mathbb{Z}/(m)$ to zero, whereas for $k = n$, it is injective, because of $\text{GCD}(m, n) = 1$. For every additive homomorphism $\psi : \mathbb{Z}/(m) \rightarrow \mathbb{Z}/(n)$ and all $x \in \mathbb{Z}/(m)$, we have $m \cdot \psi(x) = \psi(m \cdot x) = \psi(0) = 0$ in $\mathbb{Z}/(n)$. This forces $\psi(x) = 0$, because multiplication by m is injective in $\mathbb{Z}/(n)$.

Exercise 14.1 The same arguments as in [Exercise 5.8](#) on p. 106.

Exercise 14.8 If $\lambda_1 m_1 = 0$ and $\lambda_2 m_2 = 0$ for some nonzero $\lambda_{1,2} \in K$, then $\lambda_1 \lambda_2 (m_1 \pm m_2) = 0$ and $\lambda_1 \lambda_2 \neq 0$, because K has no zero divisors. Finally, $\forall \mu \in K$ $\lambda_1 (\mu m_1) = \lambda_2 (\mu m_2) = 0$.

Exercise 14.11 Let $\lambda' = \lambda + x$ and $a' = a + v$ for some $x \in I$, $v \in IM$. Then $\lambda'a' = \lambda a + (xa + \lambda v + xv)$, where the sum in parentheses lies in IM .

Exercise 14.16 For any subspace $U \subset V$, choose a basis E in U and complete it to some basis $E \sqcup F$ in V . Then $V = U \oplus W$, where W is the linear span of F .

Exercise 14.17 In the Grassmannian algebra $K\langle \xi_1, \xi_2, \dots, \xi_m \rangle$, consider two collections of homogeneous linear forms: $\eta = \xi \cdot A$ and $\zeta = \eta \cdot C = \xi \cdot F$, where $F = AC$. The Grassmannian monomials of degree k in η and ζ are $\eta_I = \sum_J \xi_J a_{JI}$ and $\zeta_K = \sum_L \xi_L f_{LK}$. Since $\zeta_I = \sum_J \eta_J c_{JI}$, we conclude that $f_{LK} = \sum_J a_{LJ} c_{JK}$.

Exercise 14.18 Let the resulting transformation of rows (respectively columns) in C be provided by left (respectively right) multiplication by the invertible matrix $S = S_k \cdots S_2 S_1$ (respectively by $R = R_1 \cdot R_2 \cdots R_\ell$). Then $F = S_k \cdots S_2 S_1 E$ (respectively $G = E R_1 \cdot R_2 \cdots R_\ell$).

Exercise 14.19 The equivalence of the first three conditions is evident in any reciprocal bases of \mathbb{Z}^m and L . The last two conditions are equivalent by the definition of the rank of a matrix.

Exercise 14.20 Clearly, $\varphi_n = 0$ for $n \geq m$. Let $0 \leq n < m$. If $\varphi_n(x) = 0$, then $p^n x = p^m y$ for some $y \in K$. Since K has no zero divisors, we conclude that $x = p^{m-n} y$. Conversely, if $x = p^{m-n} y$, then $p^n x = 0 \pmod{p^m}$. Therefore, $\ker \varphi_n = \text{im } \varphi_{m-n}$. Finally, the assignment $x \pmod{p^n} \mapsto p^{m-n} x \pmod{p^m}$ produces a well-defined K -linear injection $K/(p^n) \rightarrow K/(p^m)$ that isomorphically maps $K/(p^n)$ onto $\text{im } \varphi_{m-n}$.

Exercise 14.21 We can assume that $M = K/(p^m)$. In this case, $\ker \varphi_i / \ker \varphi_{i-1}$ consists of classes $[p^{n-i} x] \in K/(p^m)$ modulo classes of the form $[p^{n-i+1} y]$. Since multiplication by p annihilates them all, multiplication by the elements of the quotient $K/(p)$ is well defined in $\ker \varphi_i / \ker \varphi_{i-1}$.

Exercise 14.22 Answer: either for $r = 1$ and all $n_i = 0$, or for $r = 0$ and distinct $p_1, p_2, \dots, p_\alpha$.

Exercise 15.2 For $n = 1$, the space $\mathbb{k}[t]/(t) \simeq \mathbb{k}$ is simple. For $n > 1$, the image of multiplication by $[t]$ is a proper invariant subspace in $\mathbb{k}[t]/(t^n)$. Let $\mathbb{k}[t]/(t^n) = U \oplus W$, where U, W each goes to itself under multiplication by $[t]$. If U, W both are contained in the image of multiplication by $[t]$, then $U + W$ also is contained there and cannot coincide with V . Thus at least one of the subspaces U, W , say U , contains some class $[f]$ represented by the polynomial f with nonzero constant term.

Then $f, tf, \dots, t^{n-1}f$ are linearly independent in $\mathbb{k}[t]/(t^n)$. Hence $\dim U \geq n$ and $U = V$.

Exercise 15.3 If $V = U \oplus W$, where U, W both are F -invariant, then $V^* = \text{Ann } U \oplus \text{Ann } W$, and both subspaces $\text{Ann } U, \text{Ann } W$ are F^* -invariant. Indeed, if $\xi \in \text{Ann } U$, then $\forall u \in U, \langle F^*\xi, u \rangle = \langle \xi, Fu \rangle = 0$, because $Fu \in U$. Hence, $F^*\xi \in \text{Ann } U$.

Exercise 15.4 Write each (F_i, U_i) as formula (15.1) on p. 363 and use the uniqueness statement of Theorem 15.1 on p. 363

Exercise 15.5 The vectors g_i are computed recursively in decreasing order of indices as $g_{m-1} = h_m, g_i = h_{i+1} + Ag_{i+1}$. As for the remainder, $r = h_0 + F_v g_0 = h_0 + F_v(h_1 + F_v g_1) = h_0 + F_v(h_1 + A(h_2 + F_v g_2)) = \dots = h_0 + h_1 F_v + \dots + h_m F_v^m$.

Exercise 15.6 In the dual bases e and e^* of V and V^* , the matrices $tE - F_e$ and $tE - F_{e^*}$ are transposes of each other. Hence they have the same Smith forms (convince yourself of this!) and the same elementary divisors.

Exercise 15.7 Choose a basis compatible with the decomposition $V = U \oplus W$. In this basis, the matrix $tE - F$ has block-diagonal form $\begin{pmatrix} tE - G & 0 \\ 0 & tE - H \end{pmatrix}$. The result follows from the formula

$$\det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det A \cdot \det C,$$

valid for every $A \in \text{Mat}_n(\mathbb{k}), C \in \text{Mat}_m(\mathbb{k}), B \in \text{Mat}_{n \times m}(\mathbb{k})$ and verified by the Laplace expansion of the determinant in the first n columns.

Exercise 15.8 Let $f = t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n$. Write F for the matrix of multiplication by t in the basis $t^{n-1}, t^{n-2}, \dots, t, 1$ and expand $\det(tE - F)$ along the first column.

Exercise 15.9 Since multiplication by the product of all elementary divisors annihilates the direct sum in formula (15.1) on p. 363, we have $\chi_F(F) = 0$ for every operator F . This proves the Cayley–Hamilton identity for matrices over any field. In the greatest generality, the Cayley–Hamilton identity $\chi_A(A) = 0$ for $n \times n$ matrices $A = (a_{ij})$ can be treated as a collection of n^2 identities in the ring of polynomials with integer coefficients in n^2 variables a_{ij} . To prove them, it is enough to check that in evaluating these polynomial relations at all points of the coordinate space \mathbb{Q}^{n^2} , we get numerical identities. In other words, the Cayley–Hamilton identity for rational matrices implies the Cayley–Hamilton identity for matrices over any commutative ring.

Exercise 15.10 Since every vector $h \in H$ can be written as $h = u + q + r$, where $u \in U, q \in Q, r \in R$, the equality $h = \pi(h) = \pi(u) + \pi(r)$ holds in H . Since $\pi(u) = u \in U$ and $\pi(r) \in W$, we conclude that $U + W = H$. If $u \in U \cap W$, then $u = \pi(r)$ for some $r \in R$ and $\pi(u - r) = \pi(u) - \pi(r) = u - u = 0$. Thus, $u - r \in \ker \pi = Q$. This is possible only for $u = r = 0$. Hence, $U \cap W = 0$.

Exercise 15.11 The 1-dimensional isometry is $\pm \text{Id}$; the improper 2-dimensional isometry is the orthogonal direct sum of 1-dimensional isometries $+\text{Id}$ and $-\text{Id}$; the proper 2-dimensional isometry is a rotation.

Exercise 15.12 For $f \neq g$, the operators have different characteristic polynomials and cannot be similar.

Exercise 15.13 Let $\lambda \in \text{Spec } F$, $f(\lambda) \neq 0$, and let $v \in V$ be an eigenvector of F with eigenvalue λ . Then $f(F)v = f(\lambda) \cdot v \neq 0$.

Exercise 15.14 A nilpotent operator cannot have nonzero eigenvalues. Hence, all roots of $\chi_F(t)$ equal zero. Over an algebraically closed field, this forces $\chi_F(t) = t^m$. Conversely, if $\chi_F(t) = t^m$, then $F^m = 0$ by the Cayley–Hamilton identity.

Exercise 15.15 For example, the multiplication by t in the residue class module $\mathbb{k}[t]/(t^n)$ for $n \geq 2$.

Exercise 15.16 For instance, the rotation of the Euclidean plane \mathbb{R}^2 by 90° about the origin.

Exercise 15.18 Factorization of the characteristic polynomial

$$\chi_F(t) = \prod_{\lambda \in \text{Spec } F} (t - \lambda)^{N_\lambda}$$

satisfies Proposition 15.7 for $q_i = (t - \lambda)^{N_\lambda}$ and $\ker(\lambda \text{Id} - F)^{N_\lambda} = K_\lambda$.

Exercise 15.19 If $a^n = 0$, $b^m = 0$, and $ab = ba$, then $(\lambda a + \mu b)^{m+n-1} = 0$ by Newton's binomial formula.

Exercise 15.20 The map (15.17) is clearly \mathbb{C} -linear. The relation $s(fg) = s(f)s(g)$ can be verified separately for each $\text{jet } j_\lambda^m$. By the Leibniz rule,

$$(fg)^{(k)} = \sum_{v+\mu=k} \binom{k}{v} f^{(v)} g^{(\mu)}.$$

Therefore, the following congruences modulo $\text{mod}(t - \lambda)^m$ hold:

$$\begin{aligned} j_\lambda^m(fg) &\equiv \sum_k \frac{(t - \lambda)^k}{k!} \sum_{v+\mu=k} \frac{k!}{v!\mu!} f^{(v)}(\lambda) g^{(\mu)}(\lambda) \\ &\equiv \sum_k \sum_{v+\mu=k} \frac{f^{(v)}(\lambda)}{v!} (t - \lambda)^v \cdot \frac{g^{(\mu)}(\lambda)}{\mu!} (t - \lambda)^\mu \equiv j_\lambda^m(f) s_\lambda^m(g). \end{aligned}$$

Exercise 15.21 Over \mathbb{C} , one could use Proposition 15.9. Over an arbitrary field \mathbb{k} , the operator F with matrix $J_m(\lambda)$ equals $\lambda \text{Id} + N$, where $N^m = 0$ but $N^{m-1} \neq 0$. Then the inverse operator

$$\begin{aligned} F^{-1} &= (\lambda \text{Id} + N)^{-1} = \lambda^{-1} (\text{Id} + N/\lambda)^{-1} \\ &= \lambda^{-1} - \lambda^{-2} N + \lambda^{-3} N^2 - \cdots + (-1)^{n-1} \lambda^{-n} N^{n-1} \end{aligned}$$

equals $\lambda^{-1}\text{Id} + M$, where $M = -\lambda^{-2}N(1 - \lambda^{-1}N + \cdots)$ also has $M^m = 0$ but $M^{m-1} = \lambda^{2(1-n)}N^{n-1} \neq 0$. Therefore, the Jordan normal form of F^{-1} is exhausted by just one block $J_m(\lambda^{-1})$.

Exercise 16.3 In the language of correlations, the condition $\beta_1(u, w) = \beta_2(fu, fw)$ means that $\langle u, \beta_1 w \rangle = \langle fu, \beta_2 fw \rangle = \langle u, f^* \beta_2 fw \rangle$.

Exercise 16.4 Let $B = (b_{ij})$ be the matrix of $\beta : V \rightarrow V^*$. Then b_{ij} is equal to the i th coordinate of the covector βe_j in the basis $e^*_1, e^*_2, \dots, e^*_n$, that is, to the value of the covector βe_j on the vector $e_i = e_i^{**}$. The latter is $\beta(e_i, e_j)$.

Exercise 16.6 Answer: $\dim \text{Hom}_{\pm}(V, V^*) = n(n \pm 1)/2$. These are the dimensions of the spaces of symmetric and skew-symmetric matrices.

Exercise 16.7 E.g., $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$.

Exercise 16.8 For example, the linear span of the vectors $e_v + ie_{n+v}$, $1 \leq v \leq n$.

Exercise 16.9 If $B \in \text{Mat}_n(\mathbb{K})$ has $B^t = -B$, then $\det B = \det B^t = \det(-B) = (-1)^n \det B$.

Exercise 16.10 The dual basis is $1, -D, D^2/2, \dots, (-1)^n D^n/n!$.

Exercise 16.12 ${}^\vee(f^\vee) = (\beta^*)^{-1}((\beta)^{-1}f^*\beta)^*\beta^* = f^{**} = f$.

Exercise 16.13 The equality $\beta(u, w) = \beta(gu, gw)$ holds for all $u, w \in V$ if and only if $g^* \beta g = \beta$. The latter forces $\det g \neq 0$ and is equivalent to $\beta^{-1}g^* \beta = g^{-1}$.

Exercise 16.14 Since the canonical operator of $W_k((-1)^{k-1})$ and the canonical operator of $U_k \oplus U_k$ have the same elementary divisors, they are similar. Hence, the forms are equivalent by Theorem 16.1 on p. 401.

Exercise 16.15 Write $0 = u_0^i, u_1^i, u_2^i, \dots, u_m^i$, $1 \leq i \leq k$, for Jordan chains of some Jordan basis in V . Then the vectors u_1^i form a basis in $\text{im } \eta^{m-1}$; the vectors u_k^i for $1 \leq k < m$ form a basis in $\ker \eta^{m-1}$. By Lemma 16.3 on p. 406, every vector u_1^i is orthogonal to all vectors u_k^j with $k < m$.

Exercise 17.1 Let e_1, e_2, \dots, e_n form a basis in V and suppose $v, w \in V$ is expanded in terms of this basis as $u = \sum x_i e_i$, $w = \sum y_i e_i$. If we write q as in formula (17.2) on p. 421, we get

$$q(u+w) - q(u) - q(w) = (x+y)B(x^t + y^t) - xBx^t - yBy^t = xBy^t + yBx^t = 2xBy^t.$$

(The last equality holds because yBx^t is a 1×1 matrix and therefore is symmetric, i.e., $yBx^t = (yBx^t)^t = xB^t y^t = xBy^t$, since $B = B^t$.) The other statements are verified similarly.

Exercise 17.2 For every $v', v'' \in V$ and $u', u'' \in \ker q$, we have $\tilde{q}(v' + u', v'' + u'') = \tilde{q}(v', v'')$. Hence $q(v)$ depends only on $[v] = v \pmod{\ker q}$. If $u \in \ker q_{\text{red}}$, then $\tilde{q}_{\text{red}}([v], [u]) = \tilde{q}(v, u) = 0$ for all $v \in V$. This forces $u \in \ker q$ and $[u] = 0$.

Exercise 17.3 If $q(e_1) = q(e_2) = 0$ and $\tilde{q}(e_1, e_2) = \alpha \neq 0$, then the vectors e_1 and e_2/α form a hyperbolic basis for \tilde{q} .

Exercise 17.5 The reflection $\sigma_{f(e)}$ acts identically on $f(e)^\perp$ and maps $f(e) \mapsto -f(e) = f(-e)$. The composition $f \circ \sigma_e \circ f^{-1}$ does the same, because f^{-1} maps $f(e)^\perp \mapsto e^\perp$ for an orthogonal operator f .

Exercise 17.10 Let $\mathbb{P}(V) = \mathbb{P}(\text{Ann } \xi) \cup \mathbb{P}(\text{Ann } \eta)$ for some nonzero covectors $\xi, \eta \in V^*$. Then the quadratic form $q(v) = \xi(v)\eta(v)$ vanishes identically on V . Therefore, its polarization $\tilde{q}(u, w) = (q(u+w) - q(u) - q(w))/2$ also vanishes. Hence, the Gramian of q is zero, i.e., q is the zero polynomial. However, the polynomial ring has no zero divisors.

Exercise 17.11 Every rank-1 matrix is a product cr of some column c and some row r . For a symmetric matrix, $r = c^t$. Thus, a quadratic form of rank 1 looks like $q(x) = xcc^tx = (xc)^2$. A singular quadratic surface in \mathbb{P}_3 is either a double plane, or two crossing planes, or a cone over a smooth plane conic,¹¹ or a line, or a point. The last two cases are impossible over an algebraically closed field.

Exercise 17.12 Identify $\mathbb{P}_1 = \mathbb{P}(U)$ with the Veronese conic $C \subset \mathbb{P}_2 = \mathbb{P}(S^2U^*)$. Let σ swap some points A_1, A_2 and swap some other points B_1, B_2 on C . The lines (A_1A_2) and (B_1, B_2) on $\mathbb{P}_2 = \mathbb{P}(S^2U^*)$ cross at some point $P = \{a, b\}$. Then $a, b \in \mathbb{P}_1$ are the fixed points of σ . Indeed, the pencil of lines passing through P defines an involution on C that swaps the intersection points of the lines with C . This involution coincides with σ , because it acts on the four points A_i, B_i exactly as σ does. The fixed points of this involution are those such that the tangent lines drawn from P to C meet C , i.e., $\{a, a\}$ and $\{b, b\}$.

Exercise 17.13 Substituting $x = a + tb$ in $q(x) = 0$, we get $2\tilde{q}(a, b)t + q(b)t^2$. The root $t = 0$ gives $x = a$; the root $t = \tilde{q}(a, b)/q(b)$ for $\tilde{q}(a, b) \neq 0$ gives $x = c = q(b) \cdot a + \tilde{q}(a, b) \cdot b$.

Exercise 17.14 The conics passing through a given point $p \in \mathbb{P}_2 = \mathbb{P}(V)$ form a hyperplane in $\mathbb{P}_5 = \mathbb{P}(S^2V^*)$, because the equation $q(p) = 0$ is linear in q . Now (a) holds, because every five hyperplanes in \mathbb{P}_5 have nonempty intersection. To prove (c), note that a singular conic C is either a double line or a pair of intersecting lines. This forces some three points of any five points lying on C to be collinear. Therefore, every conic passing through five points without collinear triples is smooth. It is unique by Proposition 17.6 on p. 438. To prove (b), it remains to consider the case that some three of the five points lie on a line ℓ_1 and the remaining two points lie on the other line $\ell_2 \neq \ell_1$. In this case, the conic is forced to be $\ell_1 \cup \ell_2$.

Exercise 17.15 Since the space of quadrics in $\mathbb{P}_3 = \mathbb{P}(V)$ has dimension $\dim \mathbb{P}(S^2V^*) = 9$, every nine hyperplanes in $\mathbb{P}(S^2V^*)$ have nonempty intersection. This gives (a). To get (b), choose three points on each line and draw a quadric through them. To verify the last statement, note that there are no three mutually skew lines on a singular quadric by Exercise 17.11 on p. 437. A smooth quadric $S = Z(q)$ containing lines must be given by a hyperbolic form q . Hence, S is isomorphic to the Segre quadric. Such a quadric passing through given skew lines ℓ, ℓ', ℓ'' is unique,

¹¹That is, the union of lines (sa) , where $s \in \mathbb{P}_3$ is fixed and a runs through some smooth conic in the plane complementary to s .

because for every point $a \in \ell$, there exists a unique line $(b'b'') \ni a$ with $b' \in \ell'$, $b'' \in \ell''$. This line lies on a quadric, and the lines coming from all points $a \in \ell$ rule a quadric.

Exercise 17.16 Use Proposition 17.5 on p. 436 and prove that a nonempty smooth quadric over an infinite field cannot be covered by a finite number of hyperplanes.

Exercise 17.17 The Gramian of q in a basis c, e_1, e_2, \dots, e_n of $W = \mathbb{k} \oplus V$, where the e_i form a basis in V , has block form $\begin{pmatrix} f_0 & f_1 \\ f_1^t & f_2 \end{pmatrix}$, where $f_0 \in \mathbb{k}, f_1 \in V^*, f_2 \in S^2 V^*$. Since $\hat{q} : c \mapsto \lambda x_0$, where $\lambda \neq 0$, we conclude that $f_1 = 0, f_0 \neq 0$.

Exercise 17.20 Every point of $\text{Sing } Q \cap H_\infty$ is clearly singular for Q_∞ . Conversely, let $v \in \text{Sing } Q_\infty$ and $c \in \text{Sing } Q \setminus H_\infty$. Then $W = \mathbb{k} \cdot c \oplus \text{Ann } x_0$, and v is orthogonal to both $\text{Ann } x_0 = V$ and c . Hence, $v \in \text{Sing } Q \cap H_\infty$.

Exercise 18.1 The formal literal expressions checking associativity and distributivity identically coincide with those verifying the same rules in the field \mathbb{C} defined as the residue ring $\mathbb{R}[x]/(x^2 + 1)$.

Exercise 18.3 The equalities $F_{\mathbb{C}} w = \lambda w$ and $F_{\mathbb{C}} \bar{w} = \bar{\lambda} \bar{w}$ are conjugate, because $F_{\mathbb{C}}(w) = F_{\mathbb{C}}(\bar{w})$ for all $w \in V_{\mathbb{C}}$.

Exercise 18.6 See comments to Exercise 18.1.

Exercise 19.3 Compare with Exercise 16.4 on p. 389.

Exercise 19.5 The form $h_W w : W \rightarrow \mathbb{C}$ maps $w' \mapsto (w', w)$. The form $F^* h_W w : U \rightarrow \mathbb{C}$ maps $u \mapsto (Fu, w)$. The form $h_U F^\dagger : U \rightarrow \mathbb{C}$ maps $u \mapsto (u, F^\dagger w)$. Therefore, the coincidence $h_U F^\vee = F^* h_W$ means the equality $(Fu, w) = (u, F^\dagger w)$ for all u, w .

Exercise 19.6 The first assertion: $(zFu, w) = (Fu, \bar{z}w) = (u, F^\dagger \bar{z}w) = (u, \bar{z}F^\dagger w)$. The second: $(FGu, w) = (Gu, F^\dagger w) = (u, G^\dagger F^\dagger w)$.

Exercise 19.7 Since a unitary operator F is invertible, $(Fu, w) = (Fu, FF^{-1}w) = (u, F^{-1}w)$ for all $u, w \in W$.

Exercise 19.8 Consider $\text{Mat}_n(\mathbb{C})$ as a real vector space of dimension $2n^2$ with a basis formed by the matrices E_{ij}, iE_{ij} , where E_{ij} has 1 in the (i, j) th position and 0 in all other places. Write x_{ij}, y_{ij} for the coordinates in this basis. Then the matrix $(F_{ij}) = (x_{ij}) + i \cdot (y_{ij})$ is unitary if and only if the following quadratic equations¹² hold:

$$\sum_v (x_{vi}^2 + y_{vi}^2) = 1 \quad \text{for } 1 \leq i \leq n,$$

$$\sum_v (x_{vi}x_{vj} + y_{vi}y_{vj}) = \sum_v (y_{vi}x_{vj} - x_{vi}y_{vj}) = 0, \quad \text{for } 1 \leq i < j \leq n.$$

Hence, U_n is a closed subset in $\text{Mat}_n(\mathbb{C})$. Adding together all the equations written in the top row, we conclude that U_n is contained within a ball of radius \sqrt{n} centered at

¹²They expand the matrix equation $F^t \bar{F} = E$.

the origin. Therefore, U_n is compact. A diagonal matrix D with diagonal elements of the form $e^{i\vartheta}$ is connected with the identity matrix E by a smooth path $\gamma : [0, 1] \rightarrow U_n$ sending t to the diagonal matrix with elements $e^{it\vartheta}$. Since every $F \in U_n$ can be written as $F = CDC^{-1}$ for some $C \in U_n$ and diagonal D as above, the path $t \mapsto C \cdot \gamma(t) \cdot C^{-1}$ lies within U_n and connects E with F .

Exercise 19.9 The same arguments as in the proof of Proposition 19.3 on p. 492. The only difference is that now $\text{Spec } F_{\mathbb{C}}$ splits into conjugate pairs of complex numbers having unit length, that is, equal to $\cos \vartheta \pm i \sin \vartheta$. The corresponding v_1, v_2 span the Euclidean plane U , on which $F|_U$ acts as rotation through the angle ϑ .

Exercise 19.10 Arguments independent of Theorem 19.1 are sketched in Problem 19.23 on p. 502.

Exercise 19.13 Use the equality $(u, F^{\dagger}w) = (Fu, w)$.

Exercise 19.14 The proof of Theorem 19.2 works without any changes.

Exercise 19.15 For every $u = \sum x_i e_i \in U$, $F(u) = \alpha_1 x_1 f_1 + \alpha_2 x_2 f_2 + \cdots + \alpha_r x_r f_r$, because $F(e_j) = 0$ for $j > r$.

Exercise 19.16 The proof of Theorem 19.3 works without any changes.

Exercise 19.17 Write u_1, u_2, \dots, u_n and w_1, w_2, \dots, w_m for the orthonormal bases in U, W , where the matrix of the orthogonal projection $U \rightarrow W$ is as in Theorem 19.3, and let $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$ be singular values of the projection. Then $(u_i, w_i) = \alpha_i$, and all other (u_i, w_j) are equal to zero. Thus, for every $u = \sum x_i u_i$, $w = \sum x_j w_j$, $(u, w) = \sum_{i=1}^n \alpha_i x_i y_i \leq \alpha_1 \sum_{i=1}^n x_i y_i \leq \alpha_1 \cdot |x| \cdot |y|$ (the last inequality holds by formula (10.12) on p. 235). Therefore, $\cos \angle(u, w) = (u, w)/(|x| \cdot |y|) \leq \alpha_1 = (u_1, w_1)$.

Exercise 19.18 The coincidence of singular values together with $\dim U' = \dim U''$, $\dim W' = \dim W''$ forces $\dim(U' + W') = \dim(U'' + W'')$ and $\dim(U' \cap W') = \dim(U'' \cap W'')$. Therefore, we can simultaneously identify $U' + W'$ with $U'' + W''$, $U' \cap W'$ with $U'' \cap W''$, and W' with W'' by an isometry of the ambient space. It remains to remove the discrepancy of U' , U'' within the orthogonal complement to $U' \cap W' = U'' \cap W''$ taken in $U' + W' = U'' + W''$. Thus, we can assume that the ambient space is $W \oplus W^{\perp}$, where $W = W' = W''$, and the subspaces $U', U'' \subset W \oplus W^{\perp}$ are complementary to W . Such subspaces $U \subset W \oplus W^{\perp}$ are in bijection with the linear maps $F : W^{\perp} \rightarrow W$: the map F matches its graph $U = \{(v, Fv) \mid v \in W^{\perp}\}$ and is recovered from U as $F = \pi \circ \pi_{\perp}^{-1}$, where $\pi : U \rightarrow W$ is the projection along W^{\perp} , and $\pi_{\perp} : U \simeq W^{\perp}$ is the projection¹³ along W . The subspaces $U', U'' \subset W \oplus W^{\perp}$ lie in the same orbit of the action $O(W) \times O(W^{\perp}) \subset O(W \oplus W^{\perp})$ if and only if the corresponding operators $F', F'' : W^{\perp} \rightarrow W$ satisfy $F' = SF''T$ for some $T \in O(W^{\perp})$, $S \in O(W)$. By Corollary 19.5, the latter means that the singular values of F' and F'' coincide. It remains to note that if we write the matrix of the orthogonal projection $\pi : U \rightarrow W$ and the matrix of the operator $F_U : W^{\perp} \rightarrow W$ in the same basis of W and those bases in U and W^{\perp} that go to

¹³It is one-to-one, since $W \cap U = 0$.

each other under the orthogonal projection $U \simeq W^\perp$, then we get exactly the same matrices.

Exercise 20.1 The nonzero elements of the Gram matrix are

$$\widetilde{\det}(E_{11}, E_{22}) = \widetilde{\det}(E_{22}, E_{11}) = 1 \quad \text{and} \quad \widetilde{\det}(E_{12}, E_{21}) = \widetilde{\det}(E_{21}, E_{12}) = -1.$$

Since for invertible matrices we have $\eta^\vee = \det(\eta)\eta^{-1}$, for such matrices we must have $(\eta\zeta)^\vee = \det(\eta\zeta)(\eta\zeta)^{-1} = \det\zeta\zeta^{-1}\eta^{-1}\det\eta = \zeta^\vee\eta^\vee$. Since the relation is linear in each matrix and invertible matrices linearly span Mat_2 , it holds for noninvertible matrices as well.

References

- [Be] Bernoulli, J.: *Ars conjectandi, opus posthumum. Accedit Tractatus de seriebus infinitis, et epistola gallicé scripta de ludo pilae reticularis*. Basileae, impensis Thurnisiorum, fratrum (1713).
- [BS] Borevich, Z. I., Shafarevich, I. R.: *Number Theory*. Academic Press, New York (1966).
- [DS] Danilov, V. I., Shokurov, V. V.: “Algebraic Curves, Algebraic Manifolds and Schemes.” In *Encyclopedia of Mathematical Sciences*. Springer, Heidelberg (1994).
- [Fr] Francis, G. K.: *A Topological Picturebook*. Springer, Heidelberg (1987).
- [GLS] Gorenstein, D., Lyons, R. Solomon, R.: *The Classification of the Finite Simple Groups*. Mathematical Surveys and Monographs 40, vols. 1–6. AMS Providence, R.I. (1994–2005).
- [Hu] Humphreys, J. E.: *Linear Algebraic Groups*. Springer, Heidelberg (1975).
- [IR] Ireland, K., Rosen, M.: *A Classical Introduction to Modern Number Theory*. Springer, Heidelberg (1990).
- [Mu] Mumford, D.: *Tata Lectures on Theta I*. Progress in Math, vol. 23, Birkhäuser (1983).
- [Se] Serre, J.-P.: *Lie Groups and Lie Algebras: 1964 Lectures Given at Harvard University*. Lecture Notes in Mathematics series 2, vol. 1500, Springer (1965).

Index

- abelian group, [13](#), [21](#)
- absolute value of complex number, [56](#)
- action of group, [294](#)
 - diagonal, [305](#)
 - exact, [294](#)
 - faithful, [294](#)
 - free, [294](#)
 - m -transitive, [294](#)
 - transitive, [294](#)
- addition, [19](#)
 - of vectors, [22](#), [124](#)
- adjoint
 - action, [295](#)
 - linear map, [252](#), [399](#), [400](#), [487](#)
 - operator, [400](#), [411](#)
 - differential, [490](#)
 - left, [399](#)
 - right, [399](#)
- adjunct matrix, [220](#), [455](#)
- adjunction of root, [53](#)
- affine
 - algebraic
 - hypersurface, [262](#)
 - variety, [262](#)
 - chart, [253](#)
 - coordinate system, [143](#)
 - equivalence of quadrics, [444](#)
 - group, [148](#)
 - line, [146](#)
 - map, [148](#)
 - plane, [146](#)
 - quadric, [444](#)
 - cone, [449](#)
 - cylinder, [450](#)
 - paraboloid, [448](#)
 - smooth central, [447](#)
 - space, [142](#)
 - subspace, [145](#)
- affinization, [143](#)
- algebra
 - associative, [173](#)
 - commutative, [173](#)
 - finitely generated, [109](#)
 - of endomorphisms, [174](#)
 - of matrices, [178](#)
 - of quaternions, [505](#)
 - over a field, [173](#)
 - symmetric, of vector space, [259](#)
 - with division, [507](#)
 - with unit, [173](#)
- algebraic
 - closure, [55](#)
 - complement, [218](#)
 - element, [54](#), [175](#)
 - hypersurface
 - affine, [262](#)
 - projective, [263](#)
 - operation, [42](#)
 - variety
 - affine, [262](#)
 - projective, [263](#)
- algorithm
 - Euclidean division, [109](#)
 - for $\mathbb{K}[x]$, [48](#)
 - for \mathbb{Z} , [25](#)
 - Gaussian
 - elimination, [182](#), [346](#)
 - matrix inversion, [192](#)
 - Gram–Schmidt orthogonalization, [232](#), [482](#)
 - Horner’s evaluation, [47](#)
 - Kronecker’s factorization, [119](#)

- angle between
 - complex lines, 486
 - Euclidean subspaces, 498
 - hyperplanes, 243
 - vector and subspace, 243
 - vectors, 242
- anisotropic
 - quadratic form, 424
 - subspace, 424
 - vector, 424
- anti-Hermitian matrix, 467
- anti-self-adjoint
 - component of operator, 401, 488, 489
 - operator, 401, 411
- anti-self-adjoint operator
 - Euclidean, 489
 - Hermitian, 488
- antiderivative, 82
- antihomomorphism, 178, 400
- antilinear map, 463
- Appell polynomials, 89
- argument of complex number, 56
- associate elements, 111
- associated triangle, 275, 291
- associative algebra, 173
- associativity, 11, 19, 195, 279
- asymptotic
 - directions, 265, 445
 - quadric, 445
- automorphism, 3
 - inner, 295
 - of quadric, 440
 - of set, 3
 - outer, 295
- autopolar triangle, 456
- axiom
 - of choice, 12
 - of nontriviality, 20
- axis of paraboloid, 494
- barycentric
 - combination, 144
 - coordinates, 154
 - subdivision, 314, 319
- basis, 127, 132, 134, 336
 - contraoriented, 234
 - cooriented, 234
 - cyclic, 368
 - dual, 158
 - Euclidean, 236
 - Hermitian, 485
 - left, 395
 - right, 395
 - exceptional, 395, 418
 - hyperbolic, 393, 425
 - Jordan, 368, 376
 - of module, 127, 336
 - of vector space, 132, 134
 - orthogonal, 231, 423
 - orthonormal, 231, 393, 482
 - reciprocal, 344
 - semiorthonormal, 395
 - standard for K^n , 128
 - symplectic, 393
- Bernoulli numbers, 91
- bijection, 2
 - birational, 269, 438
- bilinear form, 387, 388
 - decomposable, 405
 - degenerate, 390
 - Euclidean, 393
 - Euler, 394
 - hyperbolic, 393, 425
 - indecomposable, 405
 - nondegenerate, 390
 - nonsingular, 390
 - nonsymmetric, 391
 - of type U_n , 398
 - of type $W_n(\lambda)$, 397
 - regular, 392
 - singular, 390
 - skew-symmetric, 391, 408
 - symmetric, 391, 408
 - symplectic, 393
- bilinear forms
 - equivalent, 388
 - isomorphic, 388
- bilinearity, 126
- binary
 - group of icosahedron, 517
 - operation, 19
 - quadratic form, 424
 - relation, 7
 - congruence mod n , 27
 - reflexive, 8
 - skew-symmetric, 13
 - symmetric, 8
 - transitive, 8
- binomial, 6
 - coefficient, 6, 17, 85
 - expansion, 85
 - series, 84
- biorthogonal subspaces, 405
- birational bijection, 269, 438
- Bruhat order, 322
- butterfly lemma, 325

- canonical
 - isomorphism $V \cong V^{**}$, 158
 - operator, 397
- Cantor–Schröder–Bernstein theorem, 135
- Cartesian product, 2
- Catalan numbers, 86
- Cauchy–Riemann
 - differential equations, 461
 - relations, 460
- Cauchy–Schwarz
 - Euclidean inequality, 235
 - Hermitian inequality, 483
- Cayley’s
 - parametrization, 501
 - theorem on representation of group, 294
- Cayley–Hamilton identity, 222, 340, 366
- center, 199
 - of Grassmannian algebra, 216
 - of group, 295, 330
 - of mass, 144
 - of pencil of lines, 266
- centralizer, 295
- chain in poset, 14
- characteristic, 36
 - function, 130
 - polynomial
 - of bilinear form, 392
 - of endomorphism, 226
 - of matrix, 222
 - of operator, 366
 - of recurrence relation, 82
 - value, 392
- chart affine, 253
- Chebyshev polynomials, 251
- Chinese remainder theorem, 34, 54, 120
- chirality, 513, 514
- closure, 265
- cocube, 250
- codimension, 138
- coefficient
 - binomial, 85
 - leading, 44
 - lowest, 42
 - multinomial, 5
- cofactor, 218
 - expansion, 218
- cokernel, 170
- combination
 - barycentric, 144
 - convex, 145
 - linear, 127, 130
- combinatorial type of a subspace, 191
- commensurable subgroup, 350
- commutative
 - algebra, 173
 - diagram, 168
 - ring, 21
 - reduced, 28
 - with unit, 21
 - triangle, 168
- commutativity, 19
- commutator
 - in algebra, 201
 - in group, 306
 - of matrices, 201, 385
 - subgroup, 306
- compatible elements in poset, 14
- complementary
 - subgroups, 328
 - subspaces
 - projective, 268
 - vector, 140
- complete
 - coordinate flag, 191
 - flag, 518
 - poset, 15
 - quadrangle, 274
- complex
 - conjugation, 58
 - of vectors, 463, 466
 - eigenvector, 464
 - number, 55
 - plane, 58
 - structure, 467
 - structures
 - conjugate, 478
- complex-differentiable function, 461
- complexification
 - of bilinear form, 465
 - of linear map, 463
 - of vector space, 462
- component
 - nilpotent, 379
 - of bilinear form
 - skew-symmetric, 391
 - symmetric, 391
 - of operator
 - anti-self-adjoint, 401, 488, 489
 - self-adjoint, 401, 488, 489
 - semisimple, 379
- composition, 279
 - factor, 324
 - length, 324
 - of maps, 10
 - series, 324
- cone, 449, 453

- congruence
 - modulo n , 27
 - modulo ideal, 106
 - modulo polynomial, 52
- conic, 435
- conjugate
 - complex
 - numbers, 58
 - structures, 478
 - vectors with respect to real structure, 463, 466
 - operators, 361
 - points with respect to a quadric, 443
- conjugation
 - by group element, 295
 - classes, 297
- constant term, 42
- content of polynomial, 116
- contraction, 161
- contraoriented bases, 234
- convex
 - figure, 145
 - hull, 145
- coordinate form, 156
- coordinates, 128
 - barycentric, 154
 - homogeneous, 254
 - local affine, 255
 - of vector in basis, 128
- cooriented bases, 234
- coprime
 - elements
 - in commutative ring, 26
 - in PID, 111
 - ideals, 120
 - integers, 26
 - polynomials, 48
- correlation
 - left, 389
 - right, 387
 - skew-symmetric, 391
 - symmetric, 391
- coset
 - left, 300
 - of ideal, 106
 - right, 300
- countable set, 3
- covector, 155
- Cramer's rule, 127, 223
- criterion
 - Eisenstein's, 119
 - of Krull, 122
- cross product, 507
- cross ratio, 69, 272
 - on conic, 456
- cube, 248, 283
 - group of, 292
- cycle, 281
- cyclic
 - basis, 368
 - group, 62, 281
 - operator, 370
 - permutation, 281
 - subgroup, 280
 - type
 - of linear operator, 367
 - of permutation, 282
 - vector, 370
- cyclotomic polynomial, 61, 70
- cylinder, 450
- Darboux's theorem, 410
- decomposable
 - bilinear form, 405
 - operator, 362
- decomposition
 - Jordan, 378
 - of homomorphism, 107, 149, 302
 - polar, 495
 - root, 376
 - SVD, 498
- degenerate
 - matrix, 210
 - quadratic form, 423
- degree
 - function in Euclidean domain, 109
 - lowest, 42
 - of monomial, 17
 - of polynomial, 44
 - total, 151
- dependent variables, 188
- derivative
 - logarithmic, 83
 - of a power series, 44
- Desargues's theorem, 276
- determinant, 210
 - of Gram, 233
 - of Sylvester, 227
- diagonal
 - action, 305
 - main, 197
 - matrix, 170
 - secondary, 197
- diagonalizable operator, 372
- diagram
 - Newton, 96

- Young, 6
- Young's, 17
- difference
 - of sets, 1
 - operator, 90
 - symmetric, 130
- differential
 - of affine map, 148, 445
 - of function $C \rightarrow \mathbb{C}$, 461
 - operator, 394, 490
- differentiation rules, 45
- dihedron, 284
- dimension
 - of affine space, 142
 - of vector space, 133
- direct product
 - of abelian groups, 30
 - of commutative rings, 30
 - of groups, 330
 - of sets, 2
 - of subgroups, 328
 - of vector spaces, 141
- direct sum
 - of submodules, 342
 - of vector spaces, 141
 - of vector subspaces, 140
- direction subspace, 145
- discriminant, 68
- disjoint union, 1
- distance, 238
- distributivity, 20, 195
- divisibility, 24
- division, 23
 - algebra, 507
 - of polynomials, 46
 - with remainder, 109
- dodecahedron, 283
 - group of, 293
- domain
 - Euclidean, 109
 - integral, 28
 - principal ideal, 109
 - unique factorization, 112
- double
 - line, 437
 - point, 435
- dual
 - bases, 158
 - basis
 - left, 395
 - right, 395
 - linear map, 164
 - projective spaces, 276
 - vector spaces, 155, 158
- duality
 - polar, 443
 - projective, 276
- echelon
 - matrix, 183
 - pyramid, 250
- eigenspace, 372
- eigenvalue, 371
- eigenvector, 170, 371
 - complex, 464
- Eisenstein's criterion, 119
- element
 - algebraic, 54, 175
 - associate, 111
 - generating, 309, 310
 - idempotent, 39
 - identity, 23
 - inverse, 19, 279
 - invertible, 24, 174
 - irreducible, 48, 71
 - maximal in poset, 14
 - minimal in poset, 14
 - neutral, 19, 23
 - noninvertible, 24
 - of infinite order, 281
 - of torsion, 341
 - opposite, 19
 - prime, 114
 - reducible, 48, 71
 - transcendental, 175
 - unit, 19
- elementary divisors, 351, 352
 - of operator, 363
 - theorem on, 352
- elements
 - compatible, 14
 - incompatible, 14
- ellipsoid, 447, 450
 - imaginary, 447
- elliptic
 - paraboloid, 449, 451
 - quadric, 441
- empty set, 1
- endomorphism, 3
 - algebra, 174
 - Frobenius, 37
 - linear
 - diagonalizable, 170
 - normal, 252
 - of set, 3
- epimorphism, 2

- equality
 - of maps, 2
 - of power series, 41
 - of sets, 1
- equation
 - $ax + by = k$, 24
 - $z^n = a$ in \mathbb{C} , 61
 - of Markov, 419
- equidistant, 241
- equivalence, 8
 - of quadratic forms, 422
 - of quadrics, 435, 444
- equivalence relation, 8
- Euclidean
 - adjoint operator, 489
 - algorithm
 - for $\mathbb{k}[x]$, 48
 - for \mathbb{Z} , 25
 - bilinear form, 393
 - distance, 238
 - domain, 109
 - dual basis, 236
 - length of vector, 230
 - space, 229
 - structure, 229
 - standard on \mathbb{R}^n , 229
 - standard on integrable functions, 230
 - valuation, 109
 - volume, 234
- Euler's
 - bilinear form, 394
 - four-square identity, 507
 - function, 38, 39
 - φ -function, 29
 - products, 68
 - theorem
 - on residues, 38
 - on rotations, 247
 - pentagonal, 101
- evaluation
 - form, 158
 - map, 4, 108, 121
 - of polynomial, 47
- even permutation, 208
- exact sequence, 169
- exceptional basis, 395, 418
- exponential, 83
- extension of fields, 53
- factor
 - group, 302
 - ring, 107
 - set, 8
- factorial, 4
- factorization theorem
 - for integers, 27
 - for PID, 115
 - for polynomials, 48
- Fermat's little theorem, 30
- fiber of map, 2
- Fibonacci numbers, 81, 226, 382
- field, 19
 - \mathbb{C} , 55
 - \mathbb{F}_2 , of two elements, 20
 - \mathbb{Q} , of rational numbers, 20
 - \mathbb{R} , of real numbers, 21
 - algebraically closed, 55
 - extension, 53
 - finite, 63, 64
 - noncommutative, 507
 - of fractions, 75
 - of Laurent series, 76
 - of rational functions, 76
- field of fractions, 75
- finite fields, 63
- finite length group, 324
- finite-dimensional vector space, 133
- finitely generated
 - group, 310
 - module, 127, 337, 344, 352
- finitely presented group, 311
- five lemma, 169
- flag, 191, 518
- forgetful map, 5
- form
 - bilinear, 229, 387
 - decomposable, 405
 - degenerate, 390
 - Euclidean, 393
 - Euler, 394
 - hyperbolic, 393, 425
 - indecomposable, 405
 - nondegenerate, 390
 - nonsingular, 390
 - nonsymmetric, 391
 - regular, 392
 - singular, 390
 - skew-symmetric, 391, 408
 - symmetric, 229, 391, 408
 - symplectic, 393
 - positive, 229
 - quadratic, 421
 - anisotropic, 424
 - binary, 424
 - degenerate, 423
 - hyperbolic, 424, 425
 - negative, 433

- nondegenerate, 423
 - nonsingular, 423
 - over \mathbb{F}_p , 432
 - positive, 433
 - real, 433
 - singular, 423
 - sesquilinear, 469
- formal power series, 41
- formula
 - binomial, 85
 - of Burnside–Pólya–Redfield, 298
 - of Lagrange, 159
 - of orbit length, 296
 - of Taylor, 160
 - Viète’s, 67
- fraction, 9, 73
- fractional power series, 92
- Fredholm alternative, 138
- free
 - group, 309
 - module, 336
 - variable, 188
- Frobenius endomorphism, 37
- function, 2
 - characteristic, 130
 - complex-differentiable, 461
 - rational, 76
 - real-differentiable, 461
- functional, 155
- Gaussian
 - elimination, 182
 - over PID, 346
 - integers, 62, 115
 - lemma
 - on irreducible polynomials, 117
 - on quadratic residues, 40, 523
 - quadratic reciprocity law, 66
- general linear group, 174
- generating
 - elements, 310
 - series, 80
 - set, 310
- generator, 309
 - of algebra, 109
 - of cyclic group, 62, 281
 - of group, 310
- Gram
 - determinant, 233
 - of quadratic form, 423
 - matrix, 233, 389
 - of quadratic form, 422
- Gram–Schmidt orthogonalization, 232, 482
- Gramian, 233, 389
 - of quadratic form, 422
- greatest common divisor, 24, 110
 - in an arbitrary ring, 27
 - in principal ideal domain, 110
 - in unique factorization domain, 115
 - of polynomials, 48
- group, 279
 - abelian, 13, 21
 - additive, of ring, 22
 - affine, 148
 - commutative, 13
 - cyclic, 13, 62, 281
 - dihedral, 284
 - finitely
 - generated, 310
 - presented, 311
 - free, 309
 - Klein, 284
 - linear
 - affine, 148
 - general, 174, 179
 - orthogonal, 244
 - projective, 271
 - special, 214
 - symplectic, 412
 - multiplicative, of field, 22
 - of cube, 292
 - of dodecahedron, 287, 293
 - of figure
 - complete, 283
 - proper, 283
 - of finite length, 324
 - of homotheties, 290
 - of inner automorphisms, 295
 - of invertible elements, 28
 - of invertible residue classes, 28
 - of isometries, 396
 - special, 396
 - of Mathieu, 307
 - of relations, 311
 - of roots of unity, 60
 - of tetrahedron, 286
 - of transformations, 12
 - of triangle, 285
 - of units, 28
 - orthogonal, 244
 - of quadratic form, 427
 - proper, 244
 - special, 244
- p -group, 330
- Q_8 , 304
- simple, 324
- special projective, 290

- symmetric, 13
 - symplectic, 412
 - unitary, 484
 - special, 484
- group action, 294
 - adjoint, 295
 - diagonal, 305
 - exact, 294
 - faithful, 294
 - free, 294
 - m -transitive, 294
 - regular, 294
 - left regular, 294
 - right regular, 294
 - transitive, 294
- harmonic (pairs of) points, 274, 443
- harmonicity, 274
- Hermite polynomials, 251
- Hermitian
 - adjoint
 - linear map, 487
 - matrix, 466
 - operator, 488
 - dual basis, 485
 - inner product, 481
 - isometry, 483
 - length of vector, 481
 - matrix, 467, 482
 - norm, 481
 - space, 481
 - structure, 470
 - standard on \mathbb{C}^n , 470
 - standard on space of functions, 470
 - vector space, 470
 - volume, 484
- Hilbert's basis theorem, 104
- homogeneous
 - coordinates, 254
 - polynomial, 260
- homomorphism
 - of abelian groups, 31
 - of algebras, 173
 - of fields, 34
 - of groups, 279
 - of rings, 33
 - of spaces
 - with bilinear forms, 388
 - with operators, 361
 - with quadratic forms, 422
 - of K -modules, 336
 - trivial, 33
- homothety, 154
- Hopf bundle, 516
- Horner's method, 47
- hyperbola, 264
- hyperbolic
 - basis, 393, 425
 - bilinear form, 393, 425
 - paraboloid, 449, 451
 - quadratic form, 425
 - quadric, 441
 - rotation, 428
- hyperboloid, 448
 - of one sheet, 451
 - of two sheets, 448, 450
- hyperplane, 138, 241
 - at infinity, 253
 - polar, 443
- hypersurface
 - affine, 262
 - projective, 263
- icosahedron, 283
- ideal, 103
 - maximal, 107
 - prime, 108
 - principal, 103
 - trivial, 103
- idempotent, 39, 374
 - trivial, 39
- identity map, 3
- image
 - of a point, 2
 - of group homomorphism, 289
 - of map, 2
 - of ring homomorphism, 33
- imaginary
 - ellipsoid, 447
 - part, 56
 - quaternion, 506
 - vector, 463
- incompatible elements, 14
- indecomposable
 - bilinear form, 405
 - operator, 362
- index
 - of inertia
 - negative, 433
 - positive, 433
 - of prime p in $\mathcal{E}(F)$, 365
 - of quadratic form, 433
 - of subgroup, 300
- inertia
 - index
 - negative, 433

- positive, 433
 - moment, 144
- infinity, 253
- injection, 2
- inner automorphism, 295
- inner product
 - Euclidean, 229
 - Hermitian, 481
- integral domain, 28
- interpolating polynomial, 381
- intersection of sets, 1
- invariant factors, 344, 345
 - theorem, 344
- inversion in permutation, 209
- inversion number, 209, 321
- invertible
 - element of algebra, 174
 - power series, 43
- involution, 58, 153, 304, 373
 - projective, 276
- involutive permutation, 303
- irreducible
 - element of commutative ring, 48, 71
 - factorization, 112, 113
 - factors, 113
- isometry
 - for bilinear forms, 388
 - for quadratic forms, 422, 427
 - group, 396
 - Hermitian, 483
 - of hyperbolic plane, 427
- isomorphism, 2
 - of affine quadrics, 444
 - of bilinear forms, 388
 - of operators, 361
 - of projective quadrics, 435
 - of quadratic forms, 422
 - of sets, 2
- isotropic
 - subspace, 395, 425
 - vector, 424
- jet, 380
- join, 437
- Jordan
 - basis, 368, 376
 - block, 375
 - nilpotent, 368
 - chain, 368, 405
 - decomposition, 378
 - normal form, 376
- Jordan–Hölder
 - factor, 324
 - series, 324
- Kähler triples, 471
 - with given ω , 473
 - with given g , 472
- kernel
 - of bilinear form, 409
 - left, 391
 - right, 391
 - of group homomorphism, 32, 289
 - of linear map, 125
 - of ring homomorphism, 33
- Klein group, 284
- Koszul sign rule, 216
- Kronecker’s algorithm, 119
- Krull criterion, 122
- Lagrange’s
 - interpolating polynomial, 50
 - interpolation formula, 159
 - theorem
 - on index of subgroup, 300
 - on quadratic forms, 409
- Lagrangian subspace, 413
- Laguerre polynomials, 251
- Laplace
 - operator, 499
 - relations, 218
- Laurent series, 76
- law of inertia, 434
- leading
 - coefficient, 44
 - term, 44
- least common multiple, 25
- left
 - adjoint operator, 399
 - correlation, 389
 - coset, 300
 - dual basis, 395
 - inverse map, 11
 - kernel, 391
 - orthogonal, 403
 - regular action, 294
- Legendre polynomials, 251
- Legendre–Jacobi symbol, 65, 71
- Leibniz rule, 46, 201
- lemma
 - Gauss’s
 - on irreducible polynomials, 117
 - on quadratic residues, 523

- Witt's, 430
- Zassenhaus's, 325
- Zorn's, 16
- length
 - of group, 324
 - of permutation, 321
 - of vector
 - Euclidean, 230
 - Hermitian, 481
- line
 - affine, 146
 - projective, 256, 266, 271, 437
- linear
 - combination, 127, 130
 - dependence, 131
 - endomorphism
 - cyclic, 370
 - diagonalizable, 372
 - nilpotent, 170, 367
 - normal, 252
 - semisimple, 368
 - form, 155
 - fractional transformation, 271
 - functional, 155
 - group
 - general, 174
 - projective, 271
 - special, 214
 - involution, 153
 - join, 437
 - map, 102, 125, 135, 149, 151
 - adjoint, 252
 - dual, 164
 - isometric, 388
 - projective transformation, 270
 - projector, 153
 - relations, 131, 150, 337, 338, 356
 - span, 139
 - system of hypersurfaces, 266
- local affine coordinates, 255
- localization, 73
- logarithm, 83
- logarithmic derivative, 83
- lowest
 - coefficient, 42
 - degree, 42
 - term, 42
- Möbius
 - function, 39, 203
 - inversion formula, 39, 203
 - transform, 203
- map, 2
 - affine, 148
 - bijjective, 2
 - \mathbb{C} -antilinear, 463
 - forgetful, 5
 - identity, 3
 - increasing, 14
 - injective, 2
 - inverse, 12
 - left, 11
 - right, 11
 - two-sided, 12
- K -linear, 336
- linear, 88, 102, 125, 135, 149, 151
 - adjoint, 252, 488, 489
 - dual, 164
 - isometric, 244
 - orthogonal, 244
- multilinear, 261
- nondecreasing, 14
- order-preserving, 14
- orthogonal
 - improper, 244
 - proper, 244
- polar, 443
- semilinear, 463
- surjective, 2
- Markov's
 - conjecture, 420
 - equation, 419
- mass grouping theorem, 145
- Mathieu group, 307
- matrix, 129
 - adjunct, 220, 455
 - algebra, 178
 - anti-Hermitian, 467
 - antisymmetric, 227
 - degenerate, 210
 - diagonal, 170
 - Gramian, 233
 - Hermitian, 467, 482
 - nilpotent, 202
 - nondegenerate, 210
 - of linear operator, 136
 - orthogonal, 245
 - over a noncommutative ring, 196
 - reduced echelon, 183
 - shifting, 381
 - skew-Hermitian, 467
 - skew-symmetric, 252
 - standard basis, 129
 - symmetric, 252
 - symplectic, 412
 - traceless, 252

- triangular, 197
 - unipotent, 202
 - unitary, 484
 - unitriangular, 197
 - upper triangular, 252
- maximal
 - element, 14
 - ideal, 107
- median, 153
- method
 - Gauss's, 182, 346
 - Horner's, 47
 - Newton's, 96
- metric space, 238
- middle perpendicular, 242
- minimal
 - element, 14
 - polynomial
 - of algebraic element, 54
 - of an algebraic element, 175
 - of linear operator, 365
 - word, 322
- minor, 217
 - complementary, 218
- module, 124, 335
 - cyclic, 357
 - decomposable, 343
 - finitely generated, 127
 - free, 336
 - indecomposable, 343
 - Noetherian, 356
 - semisimple, 343
 - torsion-free, 341
 - unital, 124, 335
- modulus of complex number, 56
- moment, 144
- monic polynomial, 44
- monomorphism, 2
- multilinear map, 261
- multinomial coefficient, 5
- multiple root, 51
- multiplication, 19
 - of vectors by scalars, 123
- multiplicative
 - character, 39
 - subset of ring, 73
- negative
 - inertia index, 433
 - quadratic form, 433
- neighborhood, 70
- net of hypersurfaces, 266
- Newton
 - diagram, 96
 - polygon, 96
- Newton's
 - binomial
 - modulo p , 29
 - theorem, 6, 85
 - with negative exponent, 80
 - method, 96
- nilpotent, 28
 - component, 379
 - linear endomorphism, 170
 - matrix, 202
 - operator, 367
- nilradical, 121
- Noetherian ring, 104
- nondegenerate
 - matrix, 210
 - quadratic form, 423
- nonresidue, 65
- nonsingular quadratic form, 423
- nonsymmetric bilinear form, 391
- norm
 - Hermitian, 481
 - in Euclidean domain, 109
 - of algebraic number, 113
 - quaternionic, 506
- normal
 - linear endomorphism, 252
 - operator, 417
- number
 - complex, 55
 - of partitions, 101
- numbers
 - Bernoulli, 91
 - Catalan's, 86
 - Fibonacci, 81, 382
- octahedron, 283
- octaplex, 517
- odd permutation, 208
- open set in \mathbb{C} , 70
- operation
 - n -ary
 - algebraic, 42
 - binary, 19
 - n -ary, 42
- operator, 361
 - adjoint, 400, 411
 - Hermitian, 487
 - left, 399
 - right, 399
 - anti-self-adjoint, 401, 411

- canonical, 397
- completely reducible, 368
- conjugate, 361
- cyclic, 370
- decomposable, 362
- diagonalizable, 372
- idempotent, 374
- indecomposable, 362
- involutive, 373
- irreducible, 362
- Laplacian, 499
- nilpotent, 367
- normal, 417, 491, 492
- reflexive, 400
- self-adjoint, 401, 411
- semisimple, 368
- Serre's, 397
- simple, 362
- symplectic, 412
- unitary, 483
- operators, similar, 361
- orbit, 296
 - length formula, 296
 - map, 296
- order
 - of element, 62
 - in additive group, 356
 - of group, 13, 280
 - of group element, 281
 - of invertible residue class, 38
 - partial, 13
 - total, 14
 - well, 15
- origin, 143
- orthogonal, 236
 - collection of vectors, 231
 - complement, 236, 409, 485
 - group, 244
 - of quadratic form, 427
 - special, 244
 - left, 403
 - map
 - Euclidean, 244
 - improper, 244
 - proper, 244
 - matrix, 245
 - polynomials, 251
 - projection, 237, 239, 409, 485
 - right, 403
- orthogonalization procedure, 232, 482
- orthonormal
 - basis, 393, 482
 - collection of vectors, 231
- outer automorphism, 295
- pairing, 160
 - perfect, 160
- Pappus's theorem, 276
- paraboloid, 448
 - elliptic, 449, 451
 - hyperbolic, 449, 451
- parallel displacement, 142
- parity of permutation, 209
- partial
 - fraction expansion, 77
 - order, 13
- partition, 6
 - number, 101
- pencil
 - of correlations, 391
 - of hypersurfaces, 266
- perfect
 - pairing, 160
 - square, 115, 268, 437
- permutation
 - cyclic, 281
 - even, 208
 - involutive, 303
 - odd, 208
 - shuffle, 210
- perpendicular
 - hyperplane, 241
 - middle, 242
 - vectors, 230
- perspective triangles, 276
- Pfaffian, 414
- p -group, 330
- planarity, 440
- plane
 - affine, 146
 - projective, 437
- Platonic solid, 283
- Plücker's
 - quadric, 457
 - relations, 227
- point
 - double, 435
 - singular, 435
 - smooth, 435
- polar, 443
 - decomposition, 495
 - duality, 443
 - hyperplane, 443
 - map, 443
- polarity, 443
- polarization of quadratic form, 422
- pole, 443
- polynomial, 43
 - Appell, 89

- characteristic, 222, 366
 - of bilinear form, 392
 - of endomorphism, 226
 - of recurrence relation, 82
- Chebyshev, 251
- constant, 44
- cyclotomic, 61, 70
- harmonic, 499
- Hermite, 251
- homogeneous, 260
- integer-valued, 359
- interpolating, 50, 381
- Laguerre, 251
- Legendre, 251
- minimal, 54, 175, 365
- monic, 44
- on vector space, 260
- reciprocal, 417
- reduced, 44
- separable, 51
- symmetric, 151
- polynomials
 - coprime, 48
 - orthogonal, 251
- poset, 14
 - locally finite, 202
 - totally ordered, 14
 - well ordered, 15
- positive
 - inertia index, 433
 - quadratic form, 433
- power
 - function, 84
 - series, 41
 - binomial, 84
 - generating, 80
- preimage, 2
- presentation of group, 311
- prime
 - element, 114
 - ideal, 108
 - integer, 27
 - subfield, 36
- primitive
 - residue $(\text{mod } n)$, 38
 - root
 - $(\text{mod } n)$, 38
 - of unity, 60
- principal
 - axis of paraboloid, 494
 - ideal, 103
 - domain, 109
- principle
 - Dirichlet's, 3
 - of transfinite induction, 15
- product
 - cross product, 507
 - direct
 - of abelian groups, 30
 - of commutative rings, 30
 - of groups, 330
 - of sets, 2
 - of subgroups, 328
 - direct, of vector spaces, 141
 - inner
 - Euclidean, 229
 - Hermitian, 481
 - of ideals, 120
 - of matrices, 176
 - semidirect
 - of groups, 330
 - of subgroups, 328
- projection
 - in projective space, 269
 - of conic onto line, 269, 438
 - orthogonal, 239, 409, 485
- projective
 - algebraic hypersurface, 263
 - algebraic variety, 263
 - closure, 265, 444
 - duality, 276
 - enhancement of affine quadric, 444
 - equivalence of quadrics, 435
 - line, 256
 - quadric, 435
 - root, 267
 - space, 253
 - subspace, 263
- projectivization, 253
- projector, 153, 374
- proper
 - submodule, 335
 - subset, 1
- Puiseux series, 92
- pullback of linear forms, 165
- pure imaginary
 - quaternion, 506
 - vector, 463
- Pythagorean theorem, 231
- quadrangle, 291
- quadratic
 - form, 421
 - anisotropic, 424
 - binary, 424
 - degenerate, 423
 - hyperbolic, 424, 425

- negative, 433
- nondegenerate, 423
- nonsingular, 423
- over \mathbb{F}_p , 432
- positive, 433
- real, 433
- singular, 423
- nonresidue, 65
- reciprocity, 66, 71, 225
- residue, 65
- surface, 435
- quadric
 - affine, 444
 - cone, 449
 - cylinder, 450
 - paraboloid, 448
 - equivalent
 - affinely, 444
 - projectively, 435
 - Plücker's, 457
 - projective, 435
 - real
 - elliptic, 441
 - hyperbolic, 441
 - projective, 441
 - Segre's, 439, 456
- quadruple of points
 - harmonic, 274
 - special, 273
- quaternion, 505
 - pure imaginary, 506
 - real, 506
- quotient
 - by group action, 296
 - group, 302
 - homomorphism, 107, 302
 - map, 8
 - of division, 110
 - by polynomial, 47
 - ring, 107
 - set, 8
 - space, 149
- radial vector, 143
- radical
 - function, 86
 - of ideal, 120
- rank
 - of bilinear form, 391
 - of free module, 343
 - of matrix, 166
 - over principal ideal domain, 359
 - of quadratic form, 423
- rational normal curve, 267
- real
 - number, 21
 - part, 56
 - quadratic form, 433
 - quaternion, 506
 - structure, 466
 - vector, 463
- real-differentiable function, 461
- realification, 459
- reciprocal
 - bases, 344
 - polynomial, 417
- reduced
 - echelon form, 183
 - polynomial, 44
- reducible element, 48, 71
- reduction
 - modulo n , 9
 - of coefficients, 118
- reflection, 246, 428
- reflexive
 - binary relation, 8
 - operator, 400
- reflexivity, 8
- regular
 - bilinear form, 392
 - polyhedron, 518
- relating set, 311
- relation
 - binary
 - equivalence, 8
 - reflexive, 8
 - skew-symmetric, 13
 - symmetric, 8
 - transitive, 8
 - group, 311
 - linear, 131, 337
 - module, 337
- relations, 109
 - of Cauchy–Riemann, 460
 - of Laplace, 218
 - of Plücker, 227
 - of Riemann, 477
- relator, 311
- remainder
 - in Euclidean domain, 110
 - of division by polynomial, 47
- representation of group, 294
- residue class
 - invertible, 28
 - modulo n , 27
 - primitive, 38
 - quadratic, 65

- modulo an ideal, 106
 - modulo polynomial, 52
- resultant, 228
- Riemann relations, 477
- right
 - adjoint operator, 399
 - coset, 300
 - dual basis, 395
 - inverse map, 11
 - kernel, 391
 - orthogonal, 403
 - regular action, 294
- ring, 195
 - commutative, 21
 - Euclidean, 109
 - reduced, 28
 - with unit, 21
 - Noetherian, 104
 - of fractions, 73
 - of Gaussian integers, 62
 - unique factorization domain, 112
 - with unit, 195
- root
 - adjunction, 53
 - decomposition, 376
 - of polynomial, 50
 - m -tuple, 51
 - multiple, 51
 - simple, 51
 - of unity, 60
 - primitive, 60
 - primitive modulo n , 38
 - projective, 267
 - subspace, 376
- rotary dilation, 57
- rotation
 - Euclidean, 245, 247
 - hyperbolic, 428
- Schur's theorem, 500
- section of surjective map, 11
- segment, 145
 - in a poset, 202
- Segre's
 - embedding, 439
 - quadric, 439, 456
- selection axiom, 12
- self-adjoint
 - component of operator, 401, 488, 489
 - operator, 401, 411
 - Euclidean, 489
 - Hermitian, 488
- semiaxes of Euclidean quadric, 493
- semidirect product
 - of groups, 330
 - of subgroups, 328
- semilinear map, 463
- semiorthonormal basis, 395
- semisimple
 - component, 379
 - operator, 368
- series
 - antiderivative, 82
 - fractional power, 92
 - generating, 80
 - Puiseux, 92
- Serre's operator, 397
- sesquilinear form, 469
- set, 1
 - countable, 3
 - empty, 1
 - generating, 310
 - multiplicative, 73
 - open in \mathbb{C} , 70
 - partially ordered, 14
 - relating, 311
 - uncountable, 3
- shape of echelon matrix, 183
- shift
 - operator, 89, 394
 - transformation, 142
- shifting matrix, 381
- shortest decomposition in transpositions, 322
- shuffle permutation, 210
- Siegel upper half-space, 477
- sign of permutation, 209
- signature of quadratic form, 433
- similar operators, 361
- simple
 - cone, 449
 - group, 324
 - ratio, 69
 - root, 51
- simplex, 249, 318
- simplified fraction, 76
- singular
 - locus, 435
 - point, 435
 - quadratic form, 423
 - values, 498
 - decomposition, 497
- skew
 - Hermitian matrix, 467
 - symmetric
 - bilinear form, 391, 408

- component of bilinear form, 391
 - correlation, 391
- smooth
 - central affine quadric, 447
 - point, 435
- snake lemma, 170
- space
 - affine, 142
 - dual, 155
 - Euclidean, 229
 - Hermitian, 470
 - metric, 238
 - of hypersurfaces, 265
 - of linear relations, 150
 - of quadrics, 435
 - projective, 253
 - dual, 276
 - vector, 123
 - with bilinear form, 388
 - with operator, 361
 - as $\mathbb{k}[t]$ -module, 362
 - with quadratic form, 421, 422, 431
 - with symmetric form, 426, 430
- span, linear, 139
- spanning tree, 226
- special
 - isometry group, 396
 - linear group, 214
 - orthogonal group, 244
 - projective group, 290
 - quadruple of points, 273
 - unitary group, 484
- sphere, 248
- spinor, 513, 514
- stabilizer, 296
- standard
 - affine atlas on \mathbb{P}_n , 257
 - basis in K^n , 128
 - basis matrix, 129
- Steiner system, 306
- structure
 - complex, 467
 - Euclidean, 229
 - Hermitian, 470
 - standard on \mathbb{C}^n , 470
 - standard on space of functions, 470
 - real, 466
- subgroup, 13, 280
 - commensurable, 350
 - complementary, 328
 - cyclic, 280
 - invariant, 300
 - normal, 300
 - Sylow, 331
- submodule, 335
 - complementary, 343
 - of torsion, 341
 - proper, 335
- subset, 1
 - proper, 1
- subspace, 124
 - affine, 145
 - anisotropic, 424
 - invariant, 361
 - isotropic, 395, 425
 - Lagrangian, 413
 - λ -root, 376
 - projective, 263
- subspaces
 - biorthogonal, 405
 - complementary, 140
 - transversal, 140
- subtraction, 23
- sum
 - direct, of vector spaces, 141
 - of ideals, 120
 - of linear subspaces, 139
- support of function, 130
- surjection, 2
- SVD, 498
- Sylow
 - p -subgroup, 331
 - theorem, 331
- Sylvester's
 - determinant, 227
 - law of inertia, 434
- symmetric
 - algebra, 259
 - bilinear form, 391, 408
 - component of bilinear form, 391
 - correlation, 391
 - difference, 130
 - group, 13
 - polynomial, 151
 - power of vector space, 259
- symplectic
 - basis, 393
 - bilinear form, 393
 - group, 412
 - matrix, 412
 - operator, 412
 - unit, 393
- system
 - of linear equations, 137
 - Steiner's, 306

Taylor expansion, 160

term

leading, 44

lowest, 42

tetrahedron, 283

theorem

binomial of Newton, 6

of Cantor–Schröder–Bernstein, 135

of Capelli–Fontené–Frobenius–Kronecker–
Rouché, 166

of Cayley, 294

of Cayley–Hamilton, 222

of Darboux, 410

of Desargues, 276

of Euler

on rotations, 247

pentagonal, 101

of Fermat (little), 30

of Hilbert, basis, 104

of Lagrange

on quadratic forms, 409

on subgroup index, 300

of Pappus, 276

of Pythagoras, 231

of Rouché–Fontené, 166

of Schur, 500

of Sylow, 331

of Wilson, 39

of Zermelo, 18

on elementary divisors, 352

on invariant factors, 344

thread rule, 209

Todd’s series, 90

torsion

element, 341

submodule, 341

total

degree, 151

order, 14

trace, 201

transcendental element, 175

transfinite induction principle, 15

transformation

group, 12

linear fractional, 271

transition

functions, 257

matrix, 180

transitivity, 8

transporter, 296

transposition, 208

of matrix, 166

transversal subspaces, 140

triangle

associated with quadrangle, 275, 291

autopolar, 456

commutative, 168

inequality, 239, 483

perspective, 276

trigonometry, 58

trivial

homomorphism, 33

ideal, 103

idempotent, 39

uncountable set, 3

union of sets, 1

disjoint, 1

unique factorization domain, 112

unit, 19, 279

in an algebra, 173

in group, 279

in ring, 195

symplectic, 393

unit vector, 246

unitary

group, 484

matrix, 484

operator, 483

universal property

of free group, 310

of localization, 75

upper bound, 14

values, characteristic, 392

variable

dependent, 188

free, 188

Grassmannian, 215

variety

affine, 262

projective, 263

vector, 124

anisotropic, 424

cyclic, 370

geometric, 22

isotropic, 424

pure imaginary, 463

real, 463

space, 123

Euclidean, 229, 489,
492

finite-dimensional, 133

Hermitian, 470, 481

unit, 246

vectorization, 143

- vectors
 - collinear, 125
 - generating, 127
 - linearly dependent, 131
 - linearly independent, 130
 - linearly related, 131
 - orthogonal, 230
 - orthonormal, 231
 - proportional, 125
- Veronese
 - conic, 268
 - curve, 267
 - map, 267
- vertex
 - of paraboloid, 494
 - subspace, 435
- Viète's formulas, 67
- volume, 205
 - Euclidean, 234
 - form, 206
 - Hermitian, 484
 - of simplex, 250
- web of hypersurfaces, 266
- weight
 - of multi-index, 210
 - of Young diagram, 6
- well order, 15
- Wilson's theorem, 39
- Witt's lemma, 430
- word minimal, 322
- Young diagram, 6, 17
- Zassenhaus lemma, 325
- Zermelo's theorem, 18
- zero, 19
 - divisor, 28
 - homomorphism, 33
- zeta function of a poset, 203
- Zorn's lemma, 16